

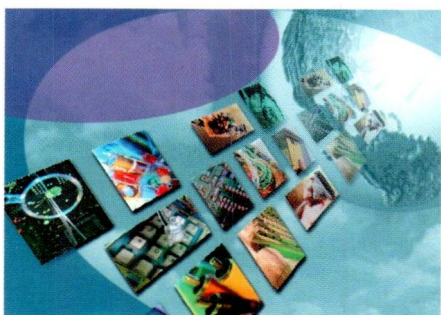
Meridian 1 and Succession Communication Server for Enterprise 1000

Remote Office **Book 1 of 2**



Meridian 1 and Succession Communication Server for Enterprise 1000

Remote Office **Book 1 of 2**



NORTEL
NETWORKS

Internet address

<http://www.nortelnetworks.com>

A0860307



NTLH02AF

Remote Office and RLC

555-8421-102

Reach Line Card

555-8421-210

Remote Office 9150

555-8421-215

P0988417

555-8421-102

Remote Office and RLC

1.3.1 Release Notes

Product release 1.3.1

Standard 1.0

October 2001

Copyright © 2001 Nortel Networks, All Rights Reserved.

Printed in Canada.

All information contained in this document is subject to change without notice. Nortel Networks reserves the right to make changes to equipment design or program components as progress in engineering, manufacturing methods, or other circumstances may warrant.

*Nortel Networks, the Nortel Networks logo, the Globemark, Unified Networks, Meridian 1, MSL-100, and Succession Communication Server for Enterprise 1000 are trademarks of Nortel Networks.

MICROSOFT, MS-DOS, WINDOWS, WINDOWS 95, WINDOWS 98, WINDOWS ME, WINDOWS 2000 and WINDOWS NT are trademarks of Microsoft Corporation.

NORTEL
NETWORKS™

Publication history

October 2001

This is the Standard 1.0 issue of the Remote Office and RLC Release Notes for Remote Office Product release 1.3.1. This release includes support for the Remote Office 911x series units, Meridian Digital Telephone IP Adapter units (Internal and External), Bridge Port, and Differentiated Services (DiffServ) along with updated Known Problems and Issues Corrected sections.

Contents

In this document

About this document	4
What's new in this release?	6
Hardware, software, and documentation requirements	9
Upgrade file names for this release	14
Performing upgrades	16
Important installation notes	18
PSTN testing	21
Bridge Ports	25
9150 BRI Configuration sheet	29
Local Remote Office 9150 unit dialing plan	30
Operation (Remote Office units)	31
Issues corrected since 1.2	34
Known problems in this release	42
Documentation additions and corrections	43

About this document

This document applies to the following firmware:

- Release 1.3.1 firmware for the RLC, Remote Office 9150 unit, Remote Office 911x series units, and Meridian Digital Telephone IP Adapter units
- Release 1.3.1 software for Configuration Manager
- Version 30d firmware for ISDN U-interface and ISDN ST-interface

Document purpose

This document describes the features, known problems, and workarounds for the Remote Office 9150 unit, Remote Office 911x series units, Meridian Digital Telephone IP Adapter units, and the Reach Line Card (RLC). It also provides:

- information that is not provided in the:
 - *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210)
 - *Remote Office 9150 Installation and Administration Guide* (NTP 555-8421-215)
 - *Remote Office 911x series Installation and Administration Guide* (NTP 555-8421-220)
 - *Meridian Digital Telephone IP Adapter Installation and Administration Guide* (NTP 555-8421-211)
- clarification for items that can prevent the system from operating correctly if they are not configured correctly (refer to “How to achieve a successful implementation” on page 5 for more details.)

Who should read this document

This document is written for individuals who are responsible for the installation, configuration, and day-to-day management of the Remote Office 9150 unit, 911x series unit, Meridian Digital Telephone IP Adapter unit, and RLC.

How to achieve a successful implementation

The instructions provided in the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210) help you achieve a successful implementation. Specifically, pay close attention to the instructions for configuring the following:

- PBX configuration for ports, DN Discovery, and Caller ID security
- PSTN numbers used to contact Remote Office units
- Prefix configuration in PSTN numbers on the RLC
- BRI trunk configuration on the Remote Office 9150 unit

Remote Office Naming Convention

Unless otherwise specified, the term “Remote Office units” refer to the following products:

- Remote Office 9110 unit
- Remote Office 9115 unit
- Remote Office 9150 unit
- Meridian Digital IP Adapter unit (Internal and External)

PBX Terminology

Throughout this document, the term “host PBX” refers to any of the following Nortel Networks PBX platforms:

- Meridian 1
- MSL-100
- Succession Communication Server for Enterprise 1000

What's new in this release?

The following major and minor feature enhancements are now supported by the Remote Office units and RLC:

Major feature enhancements

- **911x series unit support:** This release contains all of the necessary features to support up to 20 Remote Office 9110 unit(s) and Remote Office 9115 unit(s) per RLC.

This includes Digital Signal Processors (DSPs) that you can configure and the ability to place PSTN calls over an internal DSP based 14.4 modem on both the RLC and the Remote Office 911x series unit. Each RLC DSP supports four modem channels.

- **G.711 support for 911x series units:** The Remote Office 911x series unit supports the G.711 compression algorithm over IP. The Remote Office 911x series unit automatically adjusts to G.729 for QoS transition to the PSTN. This is because the Remote Office system uses a 14.4K modem for QoS transition and cannot support the 64K G.711 algorithm.
- **Meridian Digital Telephone IP Adapter (Internal and External) support:** This release contains all of the necessary features to support up to 20 Meridian Digital Telephone IP Adapters (Internal and External) per RLC.
- **Bridge port:** This feature allows local incoming PSTN calls to be handled by the Remote Office 9150 unit in a manner that allows access to the following PBX features: Transfer, Call Forward, and Conference.

Note: Since the Remote Office 911x series unit are single-port devices, they do not support the Bridge Port feature.
- **Enhanced statistics:** New statistical information is offered through the "Network statistics" screen that provides details on packet loss and other parameters related to the IP network. This screen also displays QoS transition information in a 24-hour window for each Remote Office unit. The PORTINFO and ISDNINFO fields provide statistical information on the active ports and links.

- **PSTN connectivity tests:** Allows you to verify the PSTN connection between the RLC and the Remote Office 9150 unit. Refer to “PSTN testing” on page 21.
- **Differentiated Services (DiffServ):** If enabled, this feature allows the Remote Office units to set the DiffServ code-point to Nortel Networks’ standard for Voice over IP. This standard is EF (Expedited Forwarding). It also adds and maps the 802.1p priority header to the appropriate priority. Refer to the *Remote Office Network Engineering Guidelines* (NTP 555-8421-103), *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210), and *Remote Office 9150 Installation and Administration Guide* (NTP 555-8421-215) for further details.
- **Permanent IP signaling connection:** This connection allows network administrators to set the IP signaling connection to permanent mode on the Remote Office units. This is required for environments that use Network Address Translation (NAT). Refer to the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210) for further information.

Minor feature enhancements

- **IP bandwidth:** This feature allows you to configure the maximum amount of bandwidth for the IP connection between the RLC and the Remote Office units. The RLC places calls exceeding this bandwidth over the PSTN, if PSTN is enabled. If there is insufficient PSTN bandwidth, the RLC sends a “Bandwidth Limit:” message to the digital telephone display.
- **PSTN permanent configuration moved to RLC:** The PSTN permanent configuration is now accomplished on the RLC. If there is more than one Remote Office 9150 unit on the RLC, only primary trunks need to be configured as permanent.
- **Multiple Subscriber Numbering (MSN) support:** This feature is used when each B-channel is given a separate DN numbers by the Central Office. If both DNs for the B-channels are the same, then the configuration of the first B-channel defines both B-channels.

- **Trunk support:** Due to the variations in PSTN, Remote Office provides the following capabilities:
 - **56K call establishment:** This feature has the ability to place and receive 56K calls to support data calls that carry compressed voice over the Remote Office units.
 - **56/64K dynamic adaptation:** In some carriers, 64K calls routed over a 56K infrastructure can cause errors. The dynamic adaptation feature allows the Remote Office unit and RLC to dynamically detect the limitation of the bandwidth. It is then possible to downgrade the call from 64K to 56K when routing over the 56K infrastructure.
- **Configuration Manager restart alert:** This feature alerts you to restart Configuration Manager when you have made a change to the configuration.
- **Trunk group changes:** When the Local DNs to Alert: Not Configured checkbox is selected, all telephone sets configured with Local Calling keys ring on incoming local BRI calls.
- **KBA/DBA:** Support is now available for local calling and the display of DNs for local keys defined on the Key-based Adapter (KBA) or Display-based Adapter (DBA).
- **Local Telephone (Local TCM) support for a 32-port (double-slot) RLC:** This feature allows the 32-port (double-slot) RLC to be used to support 32 local TCMs.
- **DHCP support for Remote Office 9110 unit and Remote Office 9115 unit:** Dynamic Host Control Protocol (DHCP) is now supported on the Remote Office 9110 unit and Remote Office 9115 unit.
- **ISDN line trace:** This feature is used to trace (from debug) the ISDN line in a format similar to that found in a protocol analyzer.
- **The Device information and ISDN Module information options:** These options are now available in Configuration Manager.
- **Voice Activity Detection (VAD):** This feature prevents packet transmission during periods when there is no voice data present. This can help you save bandwidth.
- **Jitter buffer target depth configuration:** The RLC's dynamic voice jitter attenuation buffer compensates for the uneven arrival of voice packets across data networks. Support is now available for configuring the size of the jitter buffer. Refer to the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210) for further details.

Hardware, software, and documentation requirements

This section identifies the following items that are required to support this release:

- supported PBX platforms and software releases
- current hardware, firmware, and software versions
- administration PC requirements
- documentation requirements

Meridian 1 software and platforms

The following Meridian 1 platforms are supported using software release 23 (or later), or are using the Enterprise Business Package:

- Options 11, 11(C) Mini, 11(E), 51(C), 61(C), 71(C), and 81(C)

Please note the platform restrictions shown in the following table:

Option 11c Mini Slot Restrictions

16-port (single-slot) RLC NTDR68xx	supported in slots 1, 2, 3 in the main chassis and 7, 8, 9, 10 in the expander chassis.
32-port (double-slot) RLC NTDR71xx	slot 1 or 2 in the main chassis (maximum of 1) and 7, 8, or 9 in the expander chassis (maximum of 2).

Since the 32-port RLC requires two backplane connections, it cannot be provisioned in slot 10 as it has only one backplane connection.

Package requirements

The following five packages are required in the X11 system software for the proper functioning of Remote Office with all Meridian 1 systems:

- package# 0 BASIC (Basic Call Processing)
- package# 19 DDSP (Digit Display)
- package# 95 CPND (Caller Party Name Display)
- package# 99 BGD (Background Terminal)
- package# 170 ARIE (Meridian Modular Sets)

Currently, all five packages are available in the Basic software bundles for all Meridian 1 systems.

MSL-100 software and platforms

The following MSL-100 platforms (using software release MSL12 or later) are supported:

- SuperNode (with series 70 Processor)
- SuperNode SE (with series 70 Processor)

Note: MSL-100 platforms require a patch to support M39xx telephones with QoS transitioning. Refer to the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210) for more information.

Hardware, software, and firmware

The following table identifies the hardware, software, and firmware supported by the Meridian 1 release.

Product	Current Nortel Product #	Minimum Nortel Product #	Current Firmware Available
RLC 16-port NA	NTDR68AC	NTDR68AA	1.3.1
RLC 32-port IPE-NA	NTDR70AC	NTDR70AA	1.3.1
RLC 32-port Opt 11-NA	NTDR71AC	NTDR71AA	1.3.1
9150-North American	NTDR69AC	NTDR69AA	1.3.1

Product	Current Nortel Product #	Minimum Nortel Product #	Current Firmware Available
9150-CALA and Asia-Pac	NTDR92AC	NTDR92AA	1.3.1
9150-Australia/New Zealand	NTDR92BC	NTDR92BA	1.3.1
RLC 16-port-Euro	NTDR68BC	NTDR68BA	1.3.1
RLC 32-port IPE-Euro	NTDR70BC	NTDR70BA	1.3.1
RLC 32-port Opt 11-Euro	NTDR71BC	NTDR71BA	1.3.1
9150-European	NTDR92CC	NTDR92CA	1.3.1
9110-Global	NTDR76BA		1.3.1
9115-Global	NTDR77BA		1.3.1
Meridian Digital Telephone Internal IP Adapter	NTDE01BA		1.3.1
Meridian Digital Telephone External IP Adapter	NTDE02BA		1.3.1
DSP Module	NTDR73AA	NTDR73AA	N/A
ISDN BRI U-interface module	NTDR74AB	NTDR74AB	30d
ISDN BRI ST-interface module	NTDR75AA	NTDR75AA	30d

	Version	Minimum Compatible Firmware	Maximum Compatible Firmware
Configuration Manager	1.3.1	1.0.1	1.3.1

Note: If you are running version 1.3.1 of Configuration Manager, you can log on to a unit with an earlier version to upgrade to the current firmware.

Remote Office 9150 ISDN BRI Interface information— for Norway and Sweden only

EN 60950:1992 Annex ZB, Special National conditions, Clause 6.2.1.2 states that in Norway and Sweden, supplementary insulation for a primary circuit is required between a Telecommunications Network Voltage (TNV) circuit and any circuit that has a connection to a protective earthing terminal.

The Remote Office 9150 unit has the ability to support up to a maximum of four ISDN BRI circuits. To comply with the specification for supplemental insulation, an isolation adapter must be placed between each of the Remote Office 9150 unit BRI inputs and the BRI lines from the service provider.

Isolation adapters are available from local vendors. You can also order the adapters from Nortel Networks as a merchandise item. The Nortel Networks part number is P0935714.

Documentation

To ensure a successful, trouble-free implementation of the RLC, Remote Office 9150 unit, Remote Office 911x series unit, and Meridian Digital Telephone IP Adapter unit into your network, have the following items on hand before you proceed:

- core documentation (confirm that you have the most up-to-date documents by checking the Nortel Networks website, as noted below under “Obtaining the documentation and training”).
 - this document
 - *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210)
 - *Remote Office 9150 Installation and Administration Guide* (NTP 555-8421-215)
 - *Remote Office 911x Series Installation and Administration Guide* (NTP 555-8421-220)
 - *Meridian Digital Telephone IP Adapter Installation and Administration Guide* (NTP 555-8421-211)

- *Remote Office Network Engineering Guidelines* (NTP 555-8421-103)

- *Remote Office Product CD-ROM* (NTDR81AE)

The *Remote Office Product CD-ROM* contains firmware and software as well as documentation in Portable Document Format (PDF).

- supplementary documents and job aids:
 - *Remote Office 911x series Quick Start Guide*
 - *Meridian Digital Telephone IP Adapter Quick Start Guide*
 - *Installer's Notes* for your hardware component (provided in the box)
 - *Remote Office and RLC Planning Forms* (available on the web)

Obtaining the documentation

To download the documentation from the web, click on the Customer Support, Documentation, and North America links at the following website:

www.nortelnetworks.com

Note: Remote Office 1.3 is a Global release.

Upgrade file names for this release

Firmware and software files are initially provided on the *Remote Office Product CD-ROM*. Upgrade files that are downloaded from the Nortel Networks website are provided in self-extracting executable files.

The following table identifies the upgrade files supported by this document for the Meridian 1 release.

Notes:

- If you are using an MSL-100 PBX, contact your Nortel Networks support representative to determine the MSL-100 upgrade file names.
- To check the current firmware follow the procedure at the bottom of page 16.

Component	Nortel Networks delivery file name	Upgrade file name
RLC	rlc1_3_1.exe	rlc-1_3_1.upg
Remote Office 9150 unit	91501_3_1.exe	9150-1_3_1.upg
Remote Office 911x series units	911x1_3_1.exe	911x-1_3_1.upg
Meridian Digital Telephone IP Adapter (Internal and External)	IPadapter1_3_1.exe	IPAdapter1_3_1.upg
ISDN BRI U-interface module	isdn30du.exe	ubri-30d.upg
ISDN BRI ST-interface module	isdn30ds.exe	sbri-30d.upg
Configuration Manager	cm1_3_1.exe	not applicable

Note: The setup.exe file provided within the cm1_3_1.exe file is used to perform the Configuration Manager upgrade.

Obtaining the latest upgrade files

If you need to upgrade the firmware or software, you can obtain the latest upgrade files from your Nortel Networks distributor or, click on the Customer Support and Software Distribution links at the following website:

www.nortelnetworks.com

Note: Remote Office 1.3 is a Global release.

Performing upgrades

WARNING

To eliminate any confusion in board numbering, the RLC automatically sets its Unit ID to 254 with this release when upgrading from releases prior to 1.2.0.

The RLC now identifies the Remote Office units by their Unit ID, not by their Unit Number or Node Name. If the Unit ID is not the same as the Unit Number in the Remote Connection Configuration on the RLC, the Unit ID in the 9150 or 911x System Configuration sheet must be changed to match the Unit Number or Node Name.

To maintain compatibility with all installations that support a single Remote Office unit, the upgrade process assigns the default Unit ID of "1" to each unit to match the default at the RLC. Following an upgrade, administrators responsible for multiple Remote Office units on a single RLC must configure the correct Unit ID at each Remote Office unit.

For complete details on performing upgrades, refer to the appropriate Installation and Administration Guide for the specific product.

ATTENTION

The protocol for communication between the RLC and the Remote Office units requires that they be running the same version in order for them to communicate with each other.

You should perform a firmware upgrade if you are using older versions of firmware (Release 1.2.x.x or earlier). To check the version of firmware you are using, do one of the following:

- If you are not connected to the device, open Configuration Manager and connect to the Remote Office unit. A window displays the RLC or Remote Office unit firmware version.
- If you are already connected to the device, choose System Information → System Data. The unit firmware version displays.

Each time you perform a firmware upgrade, the configuration database is converted (if necessary) to a format that is compatible with the new firmware. The conversion does not affect configuration settings.

To ensure that the RLC and Remote Office units do not experience communication problems during, or after the firmware upgrade, Nortel Networks recommends that you perform the upgrades as follows:

- 1 Create backup files for the Remote Office 9150, 911x, and IP Adapter units and RLC configurations. Refer to "Creating a backup configuration file" in the Nortel Networks Installation and Administration Guide for the specific product.
- 2 Upgrade the Configuration Manager software on the administration PC.
- 3 Disable the PBX slot where the RLC is installed.
- 4 Upgrade the RLC firmware.
- 5 Upgrade the Remote Office units - 9150, 911x, and IP Adapter firmware.
- 6 Remote Office 9150 units only - Upgrade the BRI module firmware for each BRI module.
- 7 Restart the RLC.
- 8 Restart all units.
- 9 Re-enable the RLC slot.

Note: The Remote Office 9150 unit's BRI module firmware must only be upgraded after the Remote Office 9150 unit's firmware is at the desired compatible level.

Important installation notes

This section provides important information about the installation of the Remote Office 9150 unit, Remote Office 911x series unit, Meridian Digital Telephone IP Adapter unit, and RLC.

Free-standing key system

Nortel Networks DOES NOT support a Remote Office system as a free-standing key system.

Automatic TELs (terminal endpoint identifiers)

BRI modules must be used in a point-to-point configuration if using automatic TEL assignments. They cannot be used in a multi-point configuration. You should also make sure that no other ISDN devices are on the line.

Flash downloads to M39xx telephone sets

Flash downloads to remote M39xx telephones can take twice as long compared to when these telephones are connected directly to a standard Nortel Networks digital line card (XDLC).

PBX and Local Feature Keys

When assigning a Local Calling key to a telephone on the Remote Office unit, ensure that the selected key does not have a feature programmed against it on the host PBX.

Multiple Appearance DNs (MADN)

Any active SCR/SCN key causes the Remote Office unit to allocate DSP and WAN bandwidth for that port. This is necessary to support a privacy over-ride feature available with the SCR/SCN key. To avoid unnecessary bandwidth from being utilized, it is recommended that MCR/MCN keys be used for MADN appearances at remote sites.

QoS transition recovery

Due to the requirement to support on-demand routers, the IP network is not continually tested during QoS transition situations. It is tested only when there are active voice calls over ISDN. As a result, transitioning needs active calls for the user-configured recovery period in order to switch back to IP.

If you are testing QoS transition by disconnecting the Ethernet cable from the Remote Office unit, or RLC, expect up to a 20 second delay before the Remote Office unit can place or receive a call. You do not encounter this delay when the network degrades and the QoS switches to BRI as designed.

Local trunk calls

Local trunk numbers cannot be pre-dialed. You must wait for the local trunk dial tone before dialing the number.

M39xx call log

When an incoming local call is answered, it is recorded in the Call Log. However, you cannot dial directly from the Call Log as the Trunk Access code and country code may not be displayed. For example, the Call Log for an ISDN number may be displayed as 4445551212, but a National code prefix (for example, 0) may also be required to dial the number and it is not shown.

Power requirement

If you want to connect the Remote Office 9150 unit to an uninterruptible power supply (UPS), ensure the UPS has a minimum of 100 Watts available.

Class of Service RING

Class of Service RING permits digital telephones to ring rather than buzz when they are offhook. Local TCM ports on the RLC support this feature, but this feature is not supported by telephone sets connected to the Remote Office units.

Local DN does not support MARP DN on the same Remote Office unit

Local calling at the Remote Office 9150 unit always results in a call being placed to the first port with the dialed number. Multiple DN appearances are not supported for local calling on the Remote Office 9150 unit.

Refer to “DN Discovery” in the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210) for further details.

MSL-100 - Telephone diagnostics on 2nd slot fails

On the MSL-100, the second slot of a double-wide card fails during diagnostic tests. You should simply ignore the diagnostic test.

Trunk to Trunk transfer gives silence

If an incoming call appears on a Local Calling key, and is transferred using the Trunk Access code to dial an outbound local call, the corresponding voice path is not established. This function is not supported.

Connecting Telephone to a port reserved for Bridge Port invalidates Bridge Port operation

Do not connect a telephone to the port that is going to be used as a Bridge Port. This can cause the Bridge Port to fail.

DN discovery cannot be configured to second slot of double-wide RLC

DN Discovery cannot be configured to use a port on the second slot of a double wide card. To solve the problem, configure the DN Discovery port on the first slot. Refer to “DN Discovery” in the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210) for further details.

PSTN testing

This is a new feature that has been developed to assist you in testing your PSTN connections.

To avoid common configuration mistakes, Nortel Networks recommends that you test the PSTN operation after you have finished configuring the PSTN numbers. In addition, you should only do PSTN testing during periods when the Remote Office unit is NOT in use.

PSTN connectivity tests work in two modes:

- Disruptive mode
- Non-disruptive mode

In both cases, you can perform the tests on a specified Remote Office unit for a specified range of data ports on the RLC. When using the disruptive mode, Nortel Networks recommends that you wait two or three minutes between tests to give the Remote Office system time to recover.

You can abort the PSTN tests at any time and the system returns to normal operation mode. The start and end of PSTN tests are recorded as display logs. To view these display logs, access Configuration Manager → Alarms/Logs/Stats → Display Logs.

WARNING

During PSTN testing, do not make any configuration changes or perform a Save to Flash on the RLC or Remote Office unit involved in the PSTN testing.

If the system reports that it cannot perform PSTN tests, determine the following:

1. Is PSTN enabled on the Remote Office unit?
2. Is the Remote Office unit enabled?

Note: You cannot perform PSTN testing on Remote Office 911x series units with both IP and PSTN enabled. During the testing, the system reports the status of the test on each port on the RLC. The meaning of the status messages are shown in the table on the following page.

No	Status Message	Comments
1	Trunk up	Link was brought up successfully to the specified number and port on the Remote Office unit side.
2	Attempt Failed	Attempt made to call specified number failed.
3	Port Busy	The specified port is in use; so, it cannot be tested.
4	No Remote Port Available	There is no Remote Office unit port available to bring up trunk on specified port.
5	Security Failed	There was a security failure while bringing up the trunk. Check security configuration settings.
6	Abnormal Failure	There is an abnormal failure on this connection due to errors on the line, or due to an emergency call on the Remote Office 9150 unit.
8	Not Closed	In non-disruptive mode, this trunk bandwidth is being used for the voice calls and so could not be freed.
9	Primary not up	If the primary trunk could not be brought up, all additional trunks show this status.
10	Primary Abnormal Fail	All additional trunks show this message if the primary trunk experiences an abnormal failure during testing.
11	Not data port	The specified port is not configured as data port.
12	Attempt by Remote Failed	Attempt by the Remote Office unit to bring up trunks from remote side failed.
13	Closed	During normal testing process, this message indicates that a trunk brought up for testing purpose is closed normally.
14	No Number to Dial	Displayed for primary if there is no PSTN number configured to dial Remote Office 9150 unit, or if the primary port is in use. Try to do test at a later time and check PSTN number configuration.
15	Primary to another unit	The specified port is primary to another Remote Office unit. No test can be performed on this port

Disruptive mode testing

If any voice calls are present on the PSTN when the testing starts, Disruptive mode testing causes all existing PSTN lines to the specified Remote Office unit to close abruptly. Before the test starts, however, the system displays a warning message indicating the number of voice calls present. You must specify that you want to go ahead with the tests.

In addition, on the Remote Office 9150 unit:

- Local trunk calls that have occupied Local and Remote configured B-channels drop.
- Remote calls occupying Remote configured B-channel calls drop.
- Local calls occupying Remote configured B-channel calls and Emergency 911 calls do not drop.
- You cannot place any local outgoing trunk calls on trunk groups that use Local and Remote B-channels.
- Similarly, no incoming local trunk calls are allowed on Local and Remote B- channels.

During disruptive mode testing, the following occurs:

- A primary channel is brought up from the RLC side.
- Other channels are tested from the:
 - RLC to the Remote Office 9150 unit
 - Remote Office 9150 unit to RLC in the given range of data ports of the RLC
- QoS transition is not allowed to happen.
- No voice calls are allowed to go on the PSTN.
- The start and end of PSTN tests are recorded as display logs. To view these display logs, access Configuration Manager → Alarms/Logs/Stats → Display Logs.
- The user can abort the PSTN tests at any time and system returns to normal operation mode.

Non-disruptive mode testing

Non-disruptive mode tests do not disturb the operation of your system. The system functions normally in that:

- calls from Remote Office units on PSTN can be made
- QoS transition occurs
- Remote Office 9150 unit local trunks calls (both incoming and outgoing) are allowed (including emergency calls)

In addition:

- You may observe that some PSTN lines brought up during the testing process do not drop automatically.
- Sometimes ports that have not been brought up during testing, but were closed due to the release of PSTN bandwidth are shown as released if they are in the given range. This depends on how many calls are placed on PSTN while the test is in progress.
- It may not be possible to test some trunks by bringing them up from the RLC or Remote Office 9150 unit and vice versa if they are in use already.

Troubleshooting

If after running the PSTN tests you encounter any PSTN failures, review the following:

- Chapter 4, “Configuring the host PBX for the RLC” in the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210)
- “Operation (Remote Office units)” on page 31

Bridge Ports

Bridge Ports provide integration between the host PBX dialing plan and the Remote Office 9150 unit local dialing plan. To determine the correct Bridge Port configuration for your particular Remote Office network, you must first consider the resource usage of both the Remote Office 9150 unit and RLC. The configuration examples below illustrate the most common resource usage scenarios in a Remote Office network. Configure a Bridge Port TN on the host PBX as a voice port. For further information, refer to the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210). For Remote Office 9150 Bridge Port configuration, refer to the *Remote Office 9150 Installation and Administration Guide* (NTP 555-8421-215).

Terminology

In the following configuration examples, a local call is defined as a call that terminates on a Local Calling key of a telephone connected to a Remote Office 9150 unit. This call can be from another local user, or an inbound call from the PSTN through the BRI circuits on the Remote Office 9150 unit. The primary DN is the first key on the Remote Office telephone set that has a DN provided by the host PBX.

Note: Bridge ports use the primary DNs of Local and Remote telephone sets connected to Remote Office 9150 units to transfer local calls to the host PBX or to conference PBX calls to local calls. The primary line key must be idle for the Bridge Port to function properly. When transferring and conferencing local calls, Bridge Port connections are established from the primary DN on the telephone set of the local call. If the DN of the telephone set connected to the Remote Office 9150 unit is in use, then the Bridge Port cannot be established.

Configuration 1

Local inbound calls ring on Remote Office telephone sets and can be forwarded or conferenced to the host PBX.

- 1 Configure and enable DN Discovery on the RLC.

Note: DN Discovery replaces the DN configured on the Local Calling key of each telephone set connected to a Remote Office 9150 unit with the same DN configured for that key on the host PBX.

- 2 Configure the Local Calling keys of each telephone set connected to a Remote Office 9150 unit as required.
- 3 Configure the BRI trunk groups to alert the required local DN's when inbound calls are received on the BRI lines.
- 4 Configure enough Bridge Ports to provide the level of call blocking desired. For example, if four inbound BRI calls are forwarded to the host PBX then you require four Bridge Ports.
- 5 Review the DSP channel requirements. Each Bridge Port call requires a DSP channel and the associated bandwidth.

When a local call is presented and answered on a Remote Office 9150 unit telephone set, you can then press the Transfer (or Conference) key. The call indicator then bounces to the primary DN key, you hear a host PBX dialtone, and you can proceed to dial.

Note: Your primary DN is used to conference a local call. The Bridge Port connects the local user to the host PBX, the Remote Office 9150 unit connects your primary DN to the host PBX, and the Conference feature on the host PBX ties it all together.

Configuration 2

Local inbound calls ring on telephone sets connected to a Remote Office 9150 unit and are forwarded to the host PBX voicemail if not answered.

- 1 Configure all items as outlined in Configuration 1 above.
- 2 Configure the telephone sets connected to the Remote Office 9150 units with Forward No Answer. Set the appropriate number of rings and enter the DN of the voicemail or voice menu service on the host PBX.

When a local call is not answered on a telephone set connected to a Remote Office 9150 unit, the Bridge Port passes the call to the host PBX voicemail. The voicemail system does NOT forward the message to the voice mailbox of the Remote Office 9150 unit user since the voicemail system and host PBX have no idea who was the original recipient of the local call. For example, the call could terminate in a corporate directory voice service, or general "after hours" voicemail box. During regular business hours, the Forward No Answer calls can reach a receptionist at the host location.

Configuration 3

All local inbound calls pass immediately to the host PBX voicemail for call treatment.

- 1 Configure and enable DN Discovery.
- 2 Configure the required number of Bridge Ports to handle the call traffic expected.
- 3 Configure the BRI trunk groups with the Local DNs to Alert fields configured to the host PBX voicemail service DN.

When placing an inbound BRI call, the bridge port connects the call to the host PBX voicemail service.

Note: If the PSTN caller uses the voicemail service to redirect the call to a Remote Office 9150 unit user, a tromboning situation occurs that uses double DSP and bandwidth resources. Ensure that the DSP and bandwidth engineering allow for this situation.

Configuration 4

All local inbound calls pass immediately to the host PBX and then redirect to the Remote Office 9150 unit user's primary DN.

- 1 Disable DN Discovery. This forces the Remote Office 9150 unit to use local DNs and does not replace the local DN with the primary DN.
- 2 Configure the required number of Bridge Ports to handle the call traffic expected.
- 3 Configure the BRI trunk groups with the Local DN to Alert fields configured to the Remote Office 9150 unit user's primary DN.

This configuration provides a local presence for a Remote Office 9150 unit user while maintaining full usage of the host PBX voicemail resources. For example, a law office could publish one of the a BRI DNs (for example, 555-1212) as a direct number. The call passes from the Bridge Port, to the host PBX and then to the primary DN on the users telephone set. If the telephone set is busy, regular call treatment occurs, including directing the call to the user's voice mailbox.

Note: This configuration creates tromboning on every call and uses double DSP and bandwidth resources. Ensure that the DSP and bandwidth engineering allow for this situation. Also, since DN Discovery is disabled, Local Switchover cannot be used and therefore all calls within the Local Office require DSP and bandwidth resources.

9150 BRI Configuration sheet

This topic provides important information about the BRI Configuration sheet. To access, go to Configuration Manager → 9150 → BRI Configuration.

Disabling Multiple Subscriber Number (MSN)

Remote Office requires the ISDN numbers to be unique per module for PSTN connections between the RLC and Remote Office 9150 unit.

Do not configure B-channels as Local and Remote if MSN is disabled.

For Remote Office 9150 units with multiple BRI modules:

- Configure a maximum of one BRI module as Remote Only if PSTN connections are required.
- Configure all other BRI modules as Local only.

For Remote Office 9150 units with just one BRI module the BRI module can be configured as Local only or Remote only. If local ISDN calls and remote calls over PSTN are required, then MSN must be enabled.

Permanent PSTN connection

When using multiple Remote Office units, you must only configure the permanent PSTN connections for the RLC's primary network ports. If you only use one Remote Office unit, you can use additional permanent PSTN connections.

Local Remote Office 9150 unit dialing plan

The Remote Office 9150 unit discovers the DN numbers of the local telephones either through DN Discovery or configuration. The Bridge Ports, Local Calling, and Local SwitchOver features depend on this knowledge as follows:

- If a call has an appearance on a Local Calling key, the Remote Office 9150 unit first attempts to complete the operation (for example, call, transfer, forward) using the local dialing plan.
- If a call is placed from a Local Calling key to a number not found in the Remote Office 9150 unit's local list, then a Bridge Port is used to place the intended call to the PBX.

Operation (Remote Office units)

This section provides important information about the operation of the Remote Office units off of a Meridian 1 or MSL-100 PBX.

ACD environments

If communication is lost to the Remote Office unit, or the unit goes offline, the ACD agent is put in Make Set Busy (MSB) mode. This mode logs the agent out of the ACD queue, so calls can be routed to other ACD agents. Once you re-establish communication, the telephone display shows "Set Busy Activated".

When an ACD agent is on a call using a Local Calling key, the Remote Office 9150 unit sends a transparent Not Ready key press to the host PBX and places the ACD agents telephone in Not Ready mode. This feature prevents the ACD agent from receiving calls when active on a local call. The Not Ready mode is removed from the telephone when the local call is terminated.

Echo cancellation

Due to the network delay introduced by the IP network, echo is more noticeable in VoIP networks than traditional networks. All echo cancellation algorithms need a small amount of time to adjust if the echo path changes. This results in the initial syllable, or word, of the first sentence having echo. After that, however, no echo is apparent.

This is a normal characteristic of the transition point between the VoIP network and traditional analog facilities. If echo is not cancelled after the beginning of the first sentence, a more serious problem (such as impedance mismatch) may be present. Also note that some environments, such as conference calls, may change the echo path. This also results in an adjustment period for Echo Cancellation.

Note: Nortel Networks Global Customer Care Services (GCCS) after investigation has discovered that the source of echo on the majority of installations is from incorrectly configured analog trunks. Please ensure that the trunks are configured correctly in the areas of trunk card type (EXUT/XUT), TIMP, and BIMP settings, and jumper settings on the actual trunk card itself. Also, measure the line loss and compensate using the trunk class of service NTC or TRC as required.

Nortel Networks recommends that the trunk card be an enhanced version (EXUT). An EXUT supports more complex impedance situations. Please refer to NTP 553-3001-106 for trunk cards and the NTP for your specific PBX for more information. Also, if you are connecting recording equipment, or Recorded Announcement (RAN) devices to an analog trunk, ensure that the trunk impedance matches the equipment impedance, or echo can occur.

Fax transmissions during Quality of Service transitions

If a QoS transition occurs while a fax is being sent or received, the packets lost prior to the transition can result in:

- a fax that is not readable at the receiving end
- error messages that appear on both the sending and receiving fax machines

If this occurs, send the fax again.

NAT routers

Translation tables within NAT routers control the communication path from the private network to the public network. Most NAT devices contain a timer that monitors the translation table entries. Each time a translation table entry is used, the timer restarts. Individual table entries are deleted if the communications path is not used and the timer expires.

It is possible, when using a Remote Office 9150 or 911x unit behind a NAT device, that prolonged periods of silence cause the NAT translation table entries to clear and drop the audio path. An example of this situation would be a remote user listening to a conference call with their telephone set on mute. After five

minutes (the default NAT translation table timer on many NAT routers) the remote user would not be able to hear the conference. The remote user can recover the audio path by going off mute and speaking into the telephone to restore the NAT table entry.

To prevent the NAT translation table from dropping the audio path:

- configure the translation tables on the NAT router with a large timer value (for example, two hours)
- configure a static translation table entry for UDP port 20480

Stutter dial tone

A stutter may be heard during a remote dial tone. This is a normal occurrence and is caused by the DSP activating a dial tone relay.

Voicemail messages and Quality of Service transitions

It can take several seconds of sustained errors to cause a Quality of Service (QoS) transition to the PSTN. During this time, voice quality may suffer due to errors. If a message to a voice mailbox is being recorded during these errors, portions of the message could be unintelligible.

When you should restart a unit

Each time you make a configuration change, you should perform a Save to Flash. Configuration Manager then prompts you to restart the unit. This ensures that all configuration changes are saved in flash memory and take effect.

Note: When you save configuration changes to Flash, the system suspends new call processing for approximately 30 seconds. Some configuration changes do not take effect until the unit has been re-started.

Issues corrected since 1.2

The following issues have been corrected since Release 1.2:

Faulty BRI module (MP08694) (PRS 1143)

When the Remote Office firmware detects a faulty BRI module, the Startup Information dialog box and Status field located on the Hardware Statistics screen now identify the module as “Faulty”. The firmware also takes the module out of service.

Profile download fails for MCAs on the MSL-100 (MP09012) (PRS 1111)

The profile download is now supported for MCAs.

Call forward issue between host and virtual TNs (MP10353) (PRS 1100)

Call forwarding between host and virtual TNs now functions properly.

No ringback or busy tone when a call is placed from the corporate directory (MP10689) (PRS 694 and PRS 974)

You can now hear a busy or ringback tone that indicates the call status on the receiving side when placing a call from the corporate directory.

Permanent BRI connection not configurable on the RLC (MP10770) (PRS 709)

In Configuration Manager, permanent BRI connections are now configured from the RLC.

Time unavailable in the caller list of M3820 telephone (MP12501) (PRS 2052)

When Caller ID was displayed on the M3820 telephone, the time and date did not also display. This has been corrected.

Key labeling (MP12742/PRS 1875 and PRS 1456)

The key labeling is now stored in Flash memory. This change preserves key labeling even after system reset.

Default product configurations lead to errors (MP13659) (PRS 2141)

The default configurations were changed to reduce customer installation errors. For example, the Remote Office 9150 unit defaults with local telephones now instead of remote telephones. This was due to an installation issue where sites with multiple Remote Office 9150 units on a single RLC were conflicting with their port registrations.

BRI firmware upgrade causes module to become unusable (MP13932) (PRS 2202)

Remote Office Product release 1.3.1 allows corrupted BRI modules to be re-programmed.

Permanent PSTN Bandwidth should be non-permanent after QoS recovery (MP13934) (PRS 2210)

In previous versions of software, setting a trunk to Permanent would mean that the Remote Office 9150 unit and RLC would leave the trunk established independent of whether it was established due to QoS reasons or was circuit-only. The code has been changed to leave the trunk up during idle times while QoS is still inadequate, but when QoS recovers, to tear down the trunk.

No message shows DN discovery runs failed or success (MP14075) (PRS 2237)

A display log has been added that indicates the completion of DN discovery and whether or not it succeeded.

Set display message "Resource Limit (x)" is not user friendly (MP14229) (PRS 2270)

The display messages now indicates:

- **Call Failure**
Call Failure indicates that an attempted call returned an error (such as, busy).
- **Bandwidth Limit**
Bandwidth limit indicates that there was not enough bandwidth available in the system to complete the requested task.
- **DSP Limit**
DSP limit indicates that there were not enough available DSP resources in the system to complete the requested task.

Set rings but cannot be answered if bandwidth is unavailable with no indication to the user as to why (MP14249) (PRS 2268)

If PSTN or DSP resources cannot be allocated, the telephone set connected to the remote unit may ring but cannot be answered. A "Resource Limit" message and Log details why this call was blocked.

Voice saturation and clipping of words (MP14595) (PRS 2308)

Occasionally, double talk can be interpreted as echo and cause the incoming voice to be clipped. The Non-Linear Processor has been improved to distinguish between echo and received voice.

Some fax machines do not work with G.729/Fax (MP14683) (PRS 2316)

Some fax machines fail when configured for G.729/Fax. These fax machines work successfully if the port is re-configured for G.711.

Headset inactivation between calls may cause alert tones to be clipped (MP14751) (PRS 2349)

The headset is now kept active when calls are in Idle status.

Local features requiring DN Discovery fail after GUI changes (MP14939) (PRS 2321)

Prior to Product release 1.3.1, port configuration changes on the Remote Office 9150 unit require DN Discovery to be rerun for local calling features to work. This has been corrected.

Only the first 4 digits from an external call are in the caller list on the M3820 telephone set (MP15147) (PRS 2352)

In some configurations of the M3820 telephone set, the Caller List only displayed the first 4 digits. This has been resolved.

ACD forced answer calls interrupt local ISDN calls (MP15661) (PRS 2353)

Local calls are no longer interrupted by ACD calls if Forced Answer is enabled.

Packet Jitter Buffer too aggressive (MP15960) (PRS 2338)

The Jitter Buffer target depth default has been changed from 30 milliseconds to 90 milliseconds and can now be configured.

Save to Flash on Configuration Wizard fails (PRS 683)

The Save to Flash option in the Configuration Wizard now functions properly.

Local ISDN calls to unused numbers may not receive audible indication (PRS 994)

Audible indications are now generated for all types of failed ISDN local calls.

Unable to use IDU command from load 32 on RLC card (PRS 1022)

The IDU command is used to gather information about the actual set connected to the Remote Office 9150 unit. After registration with the remote unit, the RLC now responds with the correct IDU information.

Registration of M3900 Release 2 telephones after a conflict (PRS 1045)

If multiple M3900 Release 2 telephones are registered for the same RLC port, a conflict may occur and the telephones may not attempt to register. To solve the problem, use SPRE codes to register and de-register.

MCAs do not work correctly if the PBX is a different companding law than the Remote Office 9150 unit (PRS 1115)

MCAs switch to a transparent mode G.711 algorithm so that they work when the Remote Office 9150 unit and RLC are set for different companding laws.

Local DN synchronization (PRS 1127)

In prior releases, after performing DN Discovery, the local DN was synchronized with the first Remote DN configured. However, if the configuration on the port was changed, the local DN was updated with the originally configured value. With this release, the local DN is always synchronized with auto-discovered DN, even if the configuration changes.

Local SwitchOver and Handsfree with M39xx telephones (PRS 1171)

Local switchover now occurs when the called party answers with handsfree on M39xx telephones.

Terminated local calls (PRS 1450)

The active local call no longer terminates when a you place a second local call by dialing the Local Call SPRE code from the remote DN.

Local call signal (PRS 873 and PRS 1473)

When there is a local call and remote signaling goes down and comes up, the display status of local call details is not affected.

Configuration Manager timing out (PRS 1525)

The Configuration Manager GUI timeout timer is reset upon any activity on the GUI. After 15 minutes of inactivity, the log in session terminates.

Local TCM ports are not functional for ports 32-47 (PRS 914 and PRS 1734)

Local TCM ports are now fully supported on the double-slot RLC.

TCP connection to the Remote Office 9150 unit (PRS 1750)

The TCP session time-out is changed so that if the IP connection is lost for 30 seconds between the administration PC and the logged in unit, Configuration Manager does not have a problem re-connecting after 30 seconds.

Help content unavailable for some statistics (PRS 1751)

The Help content is now available for the Network Statistics menu. Configuration Manager provides Help information for the Network statistics, ISDN Module statistics, and Device Information statistics.

ITONE configuration is not active after TFTP upgrade from 1.0.1 release (PRS 1791)

An issue with the order of database conversion was discovered and corrected. This now functions correctly.

QoS Transitioning voice quality (PRS 1821)

A new configuration item is added to limit voice bandwidth on the IP network. This limits the number of voice calls on the IP network, thereby increasing voice quality.

GUI should only display COM port selection for Serial connection (PRS 2046)

GUI now only displays the COM port selection for Serial connection.

GUI crashes when loading a configuration file with text wrapped at 80 characters (PRS 2097)

If a configuration record were longer than 80 characters and the capture terminal had inserted carriage returns after 80 columns, then the GUI would crash trying to read in the partial records. The GUI no longer crashes when loading a configuration file with text wrapped at 80 characters.

Only five B-channels can be programmed per trunk group (PRS 2213)

The current version of software now allows eight B-channels per trunk group.

Permanent ISDN connections will not drop using the Offline SPRE code (PRS 2304)

Permanent PSTN connections should drop when the unit goes offline. This could be achieved using the Online/Offline but not when entering the Offline SPRE code.

Loss of sidetone to agent's telephones (PRS 2312)

The handset is turned off when all calls are idle so the sidetone is lost. Press the Release key to terminate the call off of the agent telephone. Side tone is removed when the Release key is depressed.

Switching between the Call Waiting key and Local Calling key causes loss of voice on the handset (PRS 2364, previously PRS 2429)

The handset is no longer turned off when releasing a local call if the handset is offhook, resolving the loss of voice path.

Unable to make local calls on ATA (PRS 2370, previously PRS 2412)

The ATA can now place local ISDN calls.

Known problems in this release

This section describes known problems with this release and suggests solutions to these problems, if solutions are available.

M2616CT cordless telephone Local Calling keys are always activated on the base station (MP14938) (PRS 2350)

Local Calling keys are not supported on the M2616CT cordless telephone.

First call to the Remote Office 9115 unit drops after the RLC is reset (MP15765) (PRS 2339)

Allow five minutes for the Remote Office 9115 unit to re-register after the RLC is re-set before placing calls.

Some fax machines are not supported (MP15832) (PRS 2330)

Some fax machines do not support the 20Hz ring frequency of the Remote Office 9150 unit's analog port. Future releases will allow the ring frequency to be configured as 20Hz (NA standard) or 25Hz (EU standard).

M3905 telephone sets can lock up during Remote Office 9150 unit reboot (MP16241) (PRS 2457)

The M3905 telephone set receives false messages during a re-boot of the Remote Office 9150 unit and can lock up. Unplug and re-plug the telephone cord at the wall jack to recover.

Documentation additions and corrections

Supported telephone modules

Page 35 of the *Remote Office 9150 Installation and Administration Guide* (NTP 555-8421-215) includes a note stating “You cannot dial directly from the Call Log of M3900 series telephones because the Trunk Access code and country code may not be displayed”. This note is incorrect. The note should read as follows:

Note: You cannot dial host PBX calls from the Call Log of the M3900 series telephones because the Trunk Access code and country code may not be displayed. You cannot dial local calls from the Call Log of the M3900 series telephones because the information contained in the Call Log does not contain trunk group information.

Fax support

Page 47 of the *Remote Office 9150 Installation and Administration Guide* (NTP 555-8421-215) includes the following sentence:

“Faxes are sent uncompressed (that is, you require 64 Kbps of bandwidth)”.

This sentence is incorrect and should be disregarded.

Page 224 of the *Remote Office 9150 Installation and Administration Guide* (NTP 555-8421-215) provides a table that includes the following sentence:

“If G.729/Fax or G.711 compression is being used and the call is a fax call, then the fax call is sent as 64 Kbps”.

This statement is incorrect. The correct information is as follows:

- If G.729/Fax is being used and the call is a fax call, then the fax call is sent as 9600 bps.
- If G.711 (uncompressed) is being used and the call is a fax call, then the fax call is sent as 64 Kbps.

To implement a Remote Office 9150 unit behind a NAT router

Page 85 of the *Remote Office 9150 Installation and Administration Guide* (NTP 555-8421-215) describes how to implement a Remote Office 9150 unit behind a NAT router. There are several references to a “PNAT router” that should read “NAPT router”. A NAPT router is a Network Address and Port Translation router.

What to do if the telephone connection tests do not work

On page 140 and 141 of the *Remote Office 9150 Installation and Administration Guide* (NTP 555-8421-215) the section titled “What to do if the telephone connection tests do not work” does not include step 7. Step 7 should read as follows:

- 7 Use Configuration Manager to examine the display logs for errors.

Note: Refer to Configuration Manager Help for a complete listing of all display logs and the condition indicated by each.

Companding Algorithm

On page 189 of the *Remote Office 9150 Installation and Administration Guide* (NTP 555-8421-215), the field description for Companding Algorithm does not provide enough detail. The field description should read as follows:

A Companding Algorithm, or coding law, is a PCM standard by which an analog voice signal is encoded into a digital bit stream. There are two main coding laws in common use around the world, A-law and μ -law. A-law is the standard in Europe and most areas outside North American influence, while the North American and Japanese standard is μ -law (Mu-law).

In the Companding Algorithm drop down box, select the option for your Remote Office 9150 unit to override the Automatic default coding law. Select A-law or μ -law if you want the Remote Office 9150 unit to override the Automatic default coding law. Valid options are: Automatic, Mu-law, and A-law.

Note: Automatic (coding law) is the default setting. When you choose Automatic, the Remote Office 9150 unit uses the coding law configured for the ISDN BRI module in use.

For a listing of line types and their respective default coding laws, refer to “ISDN Line Type” on page 46.

Multiple Subscriber Number

On page 189 of the *Remote Office 9150 Installation and Administration Guide* (NTP 555-8421-215), the field description for Multiple Subscriber Number does not provide the correct description. The field description should read as follows:

- Click on the **Enable** option button if the Central Office provided a unique DN for each B-channel.
- Click on the **Disable** option button if the Central Office provided only one DN for both B-channels.

Configuring the Remote Office 9150 unit's IP interface

Page 195 of the *Remote Office 9150 Installation and Administration Guide* (NTP 555-8421-215) should include a reference to the QoS methods discussed in the *Remote Office Network Engineering Guidelines* (NTP 555-8421-103).

Unit ID

On Page 200 of the *Remote Office 9150 Installation and Administration Guide* (NTP 555-8421-215), the field description for Unit ID does not provide the correct description. The field description should read as follows:

The RLC's non-configurable unit ID of 254.

ISDN Line Type

On page 213 of the *Remote Office 9150 Installation and Administration Guide* (NTP 555-8421-215) the field description for ISDN Line Type does not provide enough detail. The field description should read as follows:

Select the type of ISDN line used in your country. The line type you select determines the options available in the Switch Type list box and the Automatic default coding law (Companding Algorithm) used by the ISDN BRI module being configured. To select a different coding law setting, click on the Coding Law on the 9150 System Configuration property sheet. Refer to “Companding Algorithm” on page 44 for further details.

Choose the ISDN line type according to the following table:

Line Type	Default Coding Law
Proprietary Switch	μ -law
National ISDN – 1	μ -law
National ISDN – 2	μ -law
National ISDN – 3	μ -law
National ISDN – 4	μ -law
Japan NTT	μ -law
France	A-law
Germany	A-law
ETSI EuroISDN	A-law
United Kingdom	A-law
Australia	A-law
DPNSS 1	μ -law
DASS 2	μ -law

Bridge Ports

On page 220 of the *Remote Office 9150 Installation and Administration Guide* (NTP 555-8421-215), the following incorrect paragraph appears:

You must configure Bridge Port parameters on both the RLC and Remote Office 9150 unit. For information regarding Bridge Port configuration on the RLC, refer to the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210).

The correct information is as follows:

You must configure Bridge Port parameters on both the host PBX and the Remote Office 9150 unit. For every Bridge Port defined on the Remote Office 9150 unit you must configure an SCR key with voice capability on key 0 for that port on the host PBX. For more information on configuring SCR keys on a host PBX refer to your PBX documentation.

On page 228 of the *Remote Office 9150 Installation and Administration Guide* (NTP 555-8421-215) the field description for Bridge Port should include the following notes:

- If a Remote Office 9150 unit port is configured with Bridge Port enabled, do not attach a telephone to this port.
- For a telephone set connected to a Remote Office 9150 unit with Local and Remote capability, the Bridge Port does not need to be enabled to allow you to have access to Bridge Port features.

ATA- and MCA-equipped stations and bandwidth requirements

Page 224 of the *Remote Office 9150 Installation and Administration Guide* (NTP 555-8421-215) includes a note stating "The total number of digital telephones and ATAs cannot exceed 32.". This note is incorrect. The note should read as follows:

Note: You can have up to 32 digital telephones, 1 fax machine, and 7 ATA/MCAs installed. However, only 32 simultaneous calls can be made.

Module Number

On page 290 of the *Remote Office 9150 Installation and Administration Guide* (NTP 555-8421-215), the field description for Module Number does not provide the correct field description for the Remote Office 9150 unit. The field description should read as follows:

Identifies this DSP Application Module's module number on the Remote Office 9150 unit. Valid options are: 0, 1, 2, and 3.

TELCO 2 connector pin-out table

On page 377 of the *Remote Office 9150 Installation and Administration Guide* (NTP 555-8421-215), "Fault Relay" should read "unused".

555-8421-210

Reach Line Card

Installation and Administration Guide

Product release 1.3

Standard 2.1

October 2001

NORTEL
NETWORKS

Reach Line Card

Installation and Administration Guide

Product release:	1.3
Publication number:	555-8421-210
Document release:	Standard 2.1
Date:	October 2001

Copyright © 2001 Nortel Networks. All Rights Reserved.

Printed in Canada.

All information contained in this document is subject to change without notice. Nortel Networks reserves the right to make changes to equipment design or program components, as progress in engineering, manufacturing methods, or other circumstances may warrant.

*Nortel Networks, the Nortel Networks Logo, the Globemark, Unified Networks, Meridian 1, MSL-100, and Succession Communication Server for Enterprise 1000 are trademarks of Nortel Networks.

MICROSOFT, MS-DOS, and WINDOWS are trademarks of Microsoft Corporation. PROCOMM PLUS is a trademark of Datastorm Technologies, a subsidiary of Quarterdeck Corporation.

Publication history

October 2001

This is the Standard 2.1 issue of the *Reach Line Card Installation and Administration Guide*. This issue adds support for Remote Office 911x series units and Meridian Digital Telephone IP Adapter (internal and external).

Contents

About this document	xv
About this guide	xvi
<i>How to use this guide</i>	xvi
Product overview	xvii
Skills you need	xviii
<i>Nortel Networks product knowledge</i>	xviii
<i>Telecommunications knowledge</i>	xviii
<i>Data networking knowledge</i>	xix
Conventions used in this guide	xx
<i>Precautionary messages</i>	xx
<i>Instructions for selecting menu options</i>	xx
<i>Instructions for displaying property sheets</i>	xx
<i>PBX Terminology</i>	xxi
Related information products	xxii
<i>Printed documents</i>	xxii
<i>CD-ROM</i>	xxiii

1	RLC description	1
	Product introduction	2
	<i>Physical features</i>	2
	<i>PBX hardware compatibility</i>	3
	<i>PBX software compatibility</i>	4
	<i>LED indicators</i>	7
	<i>DSP application modules (NTDR73xx)</i>	8
	<i>RLC cables</i>	9
	<i>Remote unit capacity on RLCs</i>	14
	Operational characteristics	15
	<i>Adjustable quality of service using QoS Transitioning Technology</i>	15
	<i>Port sharing options</i>	16
	<i>Multiple security levels</i>	17
	<i>Packet voice processing</i>	18
	<i>Dial-up trunking</i>	19
	<i>Bandwidth allocation</i>	22
	<i>Meridian digital telephone hardware compatibility</i>	23

How the RLC works	25
<i>RLC processing modes</i>	25
<i>9150 call scenario 1: Host-controlled mode—internal corporate call</i>	27
<i>9150 call scenario 2: Host-controlled mode—external corporate call</i>	29
<i>9150 call scenario 3: Locally controlled mode—local call</i>	31
<i>911x call scenario 1: host-controlled—corporate internal call</i>	33
<i>911x call scenario 2: host-controlled—corporate external call</i>	35
<i>911x call scenario 3: locally controlled mode—local call</i>	37
Environmental requirements	39
Power requirements	40
<i>9150 units</i>	40
<i>Remote Office 911x series and Meridian Digital Telephone</i>	
<i>IP Adapter units</i>	41

2 Planning for RLC installation 43

Preinstallation preparation	44
<i>Planning for your remote service needs</i>	44
<i>Installation planning</i>	46
<i>Deployment planning</i>	46
<i>Taking inventory</i>	47
<i>Installation checklist</i>	47
System resources management	54
<i>QoS Transitioning Technology</i>	54
<i>Host connection management</i>	54
<i>Online/offline schedule</i>	55
<i>Configurable security</i>	56
Network considerations	58
<i>IP addressing and routing</i>	58
<i>Quality of service</i>	59
<i>Trunks and dialing plans</i>	59
<i>Call blocking</i>	59
Administration PC	60
<i>Connection options</i>	60
<i>Administering multiple nodes</i>	61
<i>Windows PC requirements</i>	62
<i>Meridian Administration Tools and Configuration Manager</i>	63
Planning for future growth	64
<i>Adding DSP modules</i>	64

Deployment options	65
<i>Port and station assignment.</i>	65
<i>Implementing PSTN mode</i>	66
<i>Implementing Voice over IP mode</i>	67
<i>Implementing Quality of Service Transitioning Technology</i>	68

3 Installing the RLC 69

General safety	70
<i>Precautionary messages.</i>	70
<i>Required tools for hardware installation.</i>	70
<i>Required tools for software installation or upgrade</i>	71
Installing DSP application modules	72
<i>Determining how many DSP application modules to add.</i>	72
<i>Handling DSP application modules.</i>	72
<i>Installing DSP application modules</i>	73
Identifying the cables	74
<i>RLC Multi-I/O cable- Basic (NTDR79xx)</i>	75
<i>RLC Multi-I/O cable-Enhanced (NTDR80xx)</i>	76
Installing the Reach Line Card	78
<i>Preparing for installation</i>	78
<i>Installing an RLC</i>	78
<i>Connecting the cables to an RLC.</i>	79
Verifying the installation	81
<i>Indications of proper installation.</i>	81
<i>Indications of proper cable connections</i>	81
Configuration Manager software installation	82
<i>What's next?</i>	82
Using the Configuration Wizard to perform initial configuration	83
<i>What you can configure with the Configuration Wizard</i>	83
<i>Starting Configuration Manager</i>	84
<i>Establishing a serial connection</i>	85
<i>Performing configuration with the Configuration Wizard.</i>	88
<i>What's next?</i>	95
Testing the connections	96
<i>Check host site connections</i>	96
<i>Performing a Configuration Manager PING.</i>	97
<i>Unsuccessful PING options</i>	98
<i>What's next?</i>	99

4	Configuring the host PBX for the RLC	101
	Configuring the host trunk for a Remote Office 9150 unit.	102
	<i>ISDN PRI configuration.</i>	102
	<i>ISDN BRI configuration.</i>	103
	Configuring an RLC slot.	104
	Understanding port relationships	105
	<i>Functionality provided by the various port types</i>	105
	Configuring remote and network ports.	106
	<i>General.</i>	106
	<i>Remote port configuration.</i>	107
	<i>Network port configuration</i>	110
	<i>PBX trunks and RLC network ports.</i>	112
	<i>How the remote and network ports work together.</i>	113
	<i>MSL-100 configuration requirements</i>	113
5	Using Configuration Manager	119
	What is Configuration Manager?	120
	<i>Windows PC requirements.</i>	120
	<i>Installing Configuration Manager.</i>	120
	Starting and viewing Configuration Manager	121
	<i>System tree</i>	122
	<i>Property sheets.</i>	123
	<i>Command buttons</i>	123
	Configuration files description	125
	<i>Configuration Manager: file operations diagram</i>	125
	<i>Types of files.</i>	126
	<i>Configuration Manager: file operations description.</i>	127
	Working with configuration files	132
	<i>When to use Configuration Manager file operations.</i>	132
	<i>Creating a configuration file on the PC.</i>	133
	<i>Opening a configuration file</i>	133
	<i>Uploading a configuration to a unit</i>	134
	<i>Downloading a configuration from a unit</i>	134
	Selecting the device type for offline configuration	135
	Logging on to a unit	136
	<i>Default logon ID and password.</i>	136
	<i>Connection history.</i>	137
	<i>Auto logoff.</i>	137
	<i>Logging on to a unit using the connection history.</i>	137
	<i>Logging on to a unit using the serial port</i>	140
	Logging off of the unit	142

Performing a system restart or shutdown	143
<i>When to perform a restart or shutdown</i>	<i>143</i>
<i>Performing a system restart</i>	<i>143</i>
<i>Performing a system shutdown</i>	<i>144</i>
Closing Configuration Manager	145

6 Configuring the RLC 147

Using the XConnect command for PBX maintenance from a remote site . .	148
<i>Connecting to the host PBX's SDI port from a remote site</i>	<i>148</i>
RLC system configuration	149
<i>Voice Activity Detection</i>	<i>149</i>
<i>Jitter Buffer target depth</i>	<i>150</i>
<i>DN Discovery</i>	<i>150</i>
<i>Configuring the RLC system information</i>	<i>152</i>
<i>RLC System Configuration field descriptions</i>	<i>152</i>
Understanding the IP interface	156
<i>Reach Line Card position in your IP network</i>	<i>157</i>
IP Configuration	158
<i>Configuring the IP addresses</i>	<i>159</i>
<i>IP Configuration field descriptions</i>	<i>160</i>
<i>Prioritizing voice traffic over shared networks</i>	<i>161</i>
RLC port configuration	162
<i>Configuring an RLC port</i>	<i>164</i>
Remote Connection Configuration	171
<i>Security</i>	<i>172</i>
<i>IP connection</i>	<i>172</i>
<i>PSTN configuration</i>	<i>174</i>
<i>Special Configuration for Callback for PSTN</i>	<i>176</i>
<i>Minimum call duration timers and Idle timers</i>	<i>176</i>
<i>Configuring remote connection settings</i>	<i>177</i>
Configuring Quality of Service	182
<i>More information</i>	<i>183</i>
<i>Configuring QoS</i>	<i>183</i>
How the online/offline table works	186
<i>Online/offline configuration example</i>	<i>186</i>
<i>Online/Offline table overrides</i>	<i>187</i>
<i>Multiple offline periods</i>	<i>187</i>
<i>How the remote site goes online</i>	<i>188</i>
Online/Offline table configuration	189
<i>Configuring an Online/Offline Table</i>	<i>190</i>
Caller ID configuration	192
<i>Configuring Caller ID information</i>	<i>193</i>

DSP configuration	194
<i>Module identification</i>	195
<i>Device configuration</i>	195
<i>Configuring DSPs</i>	195

7 Administration 197

Changing the administration password	198
<i>Changing the Configuration Manager password</i>	198
<i>Changing the RLC password</i>	199
Creating a backup configuration file	200
<i>Storing backup configuration files</i>	200
<i>Creating the backup file</i>	201
Restoring the configuration	203
<i>Before you begin</i>	203
<i>Uploading a configuration file over the IP network</i>	204
Display logs	208
<i>Viewing display logs</i>	208
<i>Printing the display logs to a file</i>	209
<i>Changing the size of RLC logs</i>	210
<i>Clearing logs</i>	211
Statistics screens	212
<i>Trunk Connection Statistics</i>	212
<i>Bandwidth Connection Statistics</i>	215
<i>Caller Info Statistics</i>	218
<i>VCT Statistics</i>	221
<i>Hardware Statistics</i>	224
<i>Digital Signal Processor (DSP) Statistics</i>	228
<i>Ethernet Interface Statistics</i>	232
<i>Device Information Statistics</i>	236
<i>Network Statistics screen</i>	239
<i>PSTN Error Statistics screen</i>	242
Verifying the firmware and software version	245
<i>Verifying the software version</i>	245
<i>Verifying the firmware version</i>	246
<i>Determining the current firmware and software versions</i>	246
Obtaining the latest upgrade file	247
<i>Types of upgrades</i>	247
<i>Downloading the upgrade file</i>	247

Performing a firmware upgrade	248
<i>When to perform a firmware upgrade</i>	249
<i>About firmware upgrades and configuration files</i>	249
<i>Before you begin</i>	249
<i>Upgrading the RLC firmware</i>	250
Performing a software upgrade.	252
<i>Upgrading the Configuration Manager software</i>	252
 8 Troubleshooting	 253
Before you begin.	254
<i>Identifying why a problem occurred</i>	254
Reach Line Card LEDs.	255
<i>What to do if the LEDs do not display correctly</i>	256
Network connectivity	258
Software problems	264
<i>Display Logs definitions.</i>	265
QoS testing	266
Using Configuration Manager PING	268
<i>Performing a Configuration Manager PING.</i>	268
<i>Unsuccessful PING options</i>	270
Responding to a catastrophic failure.	271
<i>Inoperative hardware.</i>	271
Repair and warranty information	272
<i>Canada.</i>	272
<i>United States</i>	272
<i>Europe</i>	272
<i>Asia/Pacific</i>	273
<i>CALA</i>	273
 A Planning forms	 275
Completing the forms	276
Connection Information—16 ports	278
Connection Information—32 ports	283
Online/Offline Table Configuration	292
System expansion worksheet	293

B	Sample configuration files	299
	Example of a network	300
	<i>Configuration recommendation</i>	300
	<i>Network diagram</i>	301
	Voice port configuration on the Meridian 1 PBX	302
	Data port configuration for 9150 on the Meridian 1 PBX	304
	Data port configuration for 911x on the Meridian 1 PBX	306
	Voice port configuration on the MSL-100 PBX	308
	Data port configuration for 9150 on the MSL-100 PBX	310
	Data port configuration for 911x on the MSL-100 PBX	313
	RLC configuration	315
	Remote Office 9150 unit configuration	319
	Remote Office 911x series unit configuration	322
C	Pin-out tables for RLC Multi-I/O cables	323
	Reading the tables	324
	RLC Multi-I/O cable—Basic	325
	RLC Multi-I/O cable—Enhanced	327
D	Safety and regulatory information	333
	International safety compliance	334
	<i>Underwriters Laboratory (UL)</i>	334
	<i>Canadian Standards Association (CSA)</i>	334
	<i>Europe</i>	334
	<i>Australia</i>	334
	<i>Other Countries Deviations Assessed</i>	334
	Electromagnetic compatibility	335
	Electromagnetic immunity	336
	Electrostatic discharge	337
	Glossary	339
	Fields index	369
	Index	373

Preface

About this document

In this preface

About this guide	xvi
Product overview	xvii
Skills you need	xviii
Conventions used in this guide	xx
Related information products	xxii

About this guide

The *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210) is for telecom and data network managers and administrators who plan, install, and manage corporate telecommunications and data networks. This guide contains the following information:

- a detailed description of the Reach Line Card (RLC)
- procedures necessary to properly install, configure, and manage the RLC in a host PBX
- necessary configuration for the host PBX
- troubleshooting procedures for addressing possible problems

This guide assumes that you are familiar with the following:

- basic telecommunications terminology
- basic networking terminology
- PC terminology and operation (specifically, Windows 95, Windows 98, or Windows NT 4.0)
- Nortel Networks PBX terminology, functionality, and administration

How to use this guide

This guide provides step by step procedures for installing, configuring, and managing the RLC as a part of your Nortel Networks remote services network. Review this guide before beginning RLC installation and configuration.

When you are ready to begin, follow the steps for planning, installing, and configuring your hardware in the order that they are presented in this guide. This helps you to achieve a successful, trouble-free installation.

Product overview

Nortel Networks is pleased to announce the Reach Line Card (RLC). The *Reach Line Card Installation and Administration Guide* provides information on how to configure and maintain your RLC.

A standard RLC works with multiple remote service options to provide Meridian 1, MSL-100, or Succession Communication Server for Enterprise 1000 PBX functionality to telephones at one or more remote sites. These sites can be any distance from the host PBX. The RLC is compatible with Remote Office 911x series and 9150 units, and Meridian Digital Telephone Internal and External IP Adapter units.

Currently, only Meridian 1 and Succession Communication Server for Enterprise 1000 PBXs support Remote Office 911x series and Meridian Digital Telephone IP Adapters. MSL-100 PBXs do not support Remote Office 911x series or Meridian Digital Telephone IP Adapters at Remote Office Product release 1.3.

An RLC does not require external components at the host PBX location. Simply install the RLC in place of a standard Nortel Networks Extended Digital Line Card (XDLC) and configure it as if it served locally connected telephones. Channels that you do not need for remote service telephones can connect to local telephones. In this way, all channels of the RLC can provide service to your corporate telecommunications network.

To identify and locate documentation for the other elements of your Meridian network, refer to "Related information products" on page xxii.

Skills you need

Knowledge of, or experience with, the following PC concepts as appropriate to your network is helpful when administering the RLC:

- Microsoft Windows
- software installation
- network configuration

Nortel Networks product knowledge

Knowledge of, or experience with, the following Nortel Networks products and concepts:

- basic administration of a Meridian 1, MSL-100, or Succession Communication Server for Enterprise 1000 PBX (telephone set and XDLC configuration)
- characteristics and principles of XDLC operation
- PBX data calls

Telecommunications knowledge

Knowledge of, or experience with, the following aspects of telecommunications:

- digital telephone set configuration
- ISDN PRI configuration
- trunk configuration
- PBX configuration
- PBX maintenance (SDI operation)
- knowledge of RS-232 signaling

Data networking knowledge

Knowledge of, or experience with, the following aspects of data networking:

- data link (Layer 2 of the OSI model)
 - IP protocol
 - routing
- network (Layer 3 of the OSI model)
 - addressing
 - traffic analysis and provisioning
 - configuration
- Voice over IP concepts

Conventions used in this guide

This section describes the symbols and text conventions used in this guide.

Precautionary messages

Note: A “Note” describes the secondary results of procedures or commands, or special conditions where you must use a procedure or command.

ATTENTION!

Provides information essential to the completion of a task.



CAUTION

Risk of data loss or equipment damage

Cautions you against unsafe practices or potential hazards, such as equipment damage, service interruption, or loss of data.

Instructions for selecting menu options

To simplify the instructions for selecting menu options, this guide abbreviates the selection path. For example, if you must choose Telnet from the Logon Unit menu, under the Connect menu, this guide uses the following style:

From the menu, choose Connect → Logon Unit → Telnet.

Instructions for displaying property sheets

To simplify the procedures for accessing property sheets throughout this guide, the instructions for displaying a particular property sheet are summarized in a “Getting there” statement.

The procedure for displaying the screen that you need depends on if you are:

- performing an online configuration (connected to a node by Telnet)
- performing an offline configuration (not connected to a node)

Example

Getting there RLC → Configuration Manager → IP Configuration

The long instruction for this example is shown below.

- 1 Do the following:

IF	THEN
you are performing an offline configuration	select the device type as described in "Selecting the device type for offline configuration" on page 125.
you are performing an online configuration	connect to, and then log on to the node as described in "Logging on to a unit" on page 126.

- 2 In the left pane, click on the plus sign (+) beside Configuration Manager to expand the node list.
- 3 Click on **IP Configuration**.

Result: The IP Configuration property sheet for the RLC displays in the right pane.

PBX Terminology

Throughout this guide, the term "host PBX" refers to any of the following Nortel Networks PBX platforms:

- Meridian 1
- MSL-100
- Succession Communication Server for Enterprise 1000

Related information products

This section lists sources for additional information related to the RLC. You can order printed documentation and the CD-ROM from your Nortel Networks distributor.

You can also download the documentation in Portable Document Format (PDF) from the Nortel Networks website. To locate these documents, click on the Customer Support, Documentation, and North America links at the following website:

www.nortelnetworks.com

Note: The information available on the website may supersede the information provided on the CD-ROM.

For further details, refer to *Remote Office and RLC Release Notes* (NTP 555-8421-102).

Printed documents

The following documents provide additional information on the RLC and other elements of a Remote Office system:

Remote Office Network Engineering Guidelines (NTP 555-8421-103)

The *Engineering Guidelines*, written for the installer/administrator, describe how a Remote Office system integrates with existing telecommunications and data networks. This document helps you to ensure that your networks are prepared for Remote Office.

Remote Office and RLC Release Notes (NTP 555-8421-102)

The *Release Notes*, written for the installer/administrator, describe the features and known problems for the different elements of a Remote Office system. This document contains information pertaining to the Reach Line Card (RLC), the Remote Office 9150 unit, Remote Office 911x series units, and Meridian Digital Telephone IP Adapter units.

**Remote Office 9150 Installation and Administration Guide
(NTP 555-8421-215)**

The *Remote Office 9150 Installation and Administration Guide*, written for the installer/administrator, describes how to install, configure, and manage the Remote Office 9150 unit.

**Remote Office 911x Series Installation and Administration Guide
(NTP 555-8421-220)**

The *Remote Office 911x Series Installation and Administration Guide*, written for the installer/administrator, describes how to install, configure, and manage Remote Office 911x series units.

**Meridian Digital Telephone IP Adapter Installation and
Administration Guide (NTP 555-8421-211)**

The *Meridian Digital Telephone IP Adapter Installation and Administration Guide*, written for the installer/administrator, describes how to install, configure, and manage Meridian Digital Telephone IP Adapter units.

CD-ROM

A Remote Office Product CD-ROM is available containing the documentation in Portable Document Format (PDF), firmware, and Configuration Manager software.

Chapter 1

RLC description

In this chapter

Product introduction	2
Operational characteristics	15
How the RLC works	25
Environmental requirements	39
Power requirements	40

Product introduction

The RLC emulates a standard Extended Digital Line Card (XDLC) and provides Private Branch Exchange (PBX) functionality for telephones at remote locations. The RLC supports up to 20 remote devices (with a limit of four Remote Office 9150 units for a single RLC). The total number of simultaneous telephone calls cannot exceed the total number of RLC ports in the host PBX. The RLC supports the following devices:

- Remote Office 9110
- Remote Office 9115
- Remote Office 9150
- Meridian Digital Telephone Internal IP Adapter
- Meridian Digital Telephone External IP Adapter

You can configure each port on the RLC as if telephones were locally connected to a standard XDLC. Existing digital trunks (PRI) or an integrated 10BaseT Ethernet interface (Voice over IP) carry voice and signaling traffic as packets.

You can upload RLC firmware through a customer-provided trivial file transfer protocol (TFTP) server installed on the administration PC, through a 10BaseT Ethernet connection.

Physical features

The 16-port version of the RLC (NTDR68xx) provides service for up to 16 telephones. At the host location, install a 16-port RLC in an IPE shelf of the host PBX, or the Option 11 cabinet of a Meridian 1 PBX.

The 32-port version of the RLC (NTDR70xx or NTDR71xx) provides service for up to 32 telephones. At the host location, install a 32-port RLC in an IPE shelf of the host PBX, or the Option 11 cabinet of a Meridian 1 PBX.

PBX hardware compatibility

The following sections list the RLC's PBX requirements.

Meridian 1

The RLC is compatible with the following Meridian 1 systems:

- Meridian 1 Option 11, 11(C), 11(C) Mini, 11(E), 51(C), 61(C), 71(C), and 81(C)

The RLC is compatible with the 11(C)-mini with the following limitations:

- The 16-port RLC is supported in slots 1—3 in the main chassis.
- The 16-port RLC is supported in slots 7—10 in the expander chassis.
- The 32-port RLC is supported in slots 1 or 2 in the main chassis, with a maximum of one RLC.
- The 32-port RLC is supported in slots 7, 8, or 9 in the expander chassis, with a maximum of two RLCs.

Note: Since the 32-port RLC requires two backplane connections, it cannot be assigned to slot 10, because this slot provides only one backplane connection.

- Older Meridian 1 systems that are upgraded with IPE modules

Note: NT8D37AA IPE cabinets utilize split-slot wiring. If you have one of these cabinets, your RLC can only reside in slots 0, 4, 8, and 12 without rewiring the cabinet.

To use any other slot, you need to rewire part of the IPE backplane using cable NT8D81AA (A0359946). Refer to the *Meridian 1 System Installation and Maintenance Manual* (NTP 553-3001-210) for details.

MSL-100

The RLC's required packages for MSL-100 PBXs are as follows:

- X11 packages 0 and 121 contain all the four required Classes of Service.
 - Package Number 0 (Basic Call Processing Package) includes FLXA, VCE, and WTA.
 - Package Number 121 (Station Camp-on) includes CPTA.

- The following four feature sets of Release 25.30 include both packages:
 - NTSK11CQ: Option 11C General Business Feature Set
 - NTSK11DQ: Option 11C Enhanced Business Feature Set
 - NTSK11EQ: Option 11C Enterprise Business Feature Set
 - NTSK11FQ: Option 11C nas/vns Feature Set

Succession Communication Server for Enterprise 1000

To obtain the RLC requirements for Succession Communication Server for Enterprise 1000 PBXs, contact your Nortel Networks distributor.

IPE vs. Option 11

You can purchase 32-port RLCs for both IPE shelves and Option 11 cabinets. Because the dimensions of card slots in IPE shelves and Option 11 cabinets differ slightly, Nortel Networks offers two varieties of the 32-port RLC. Each variety has its own order code, as outlined in the following table:

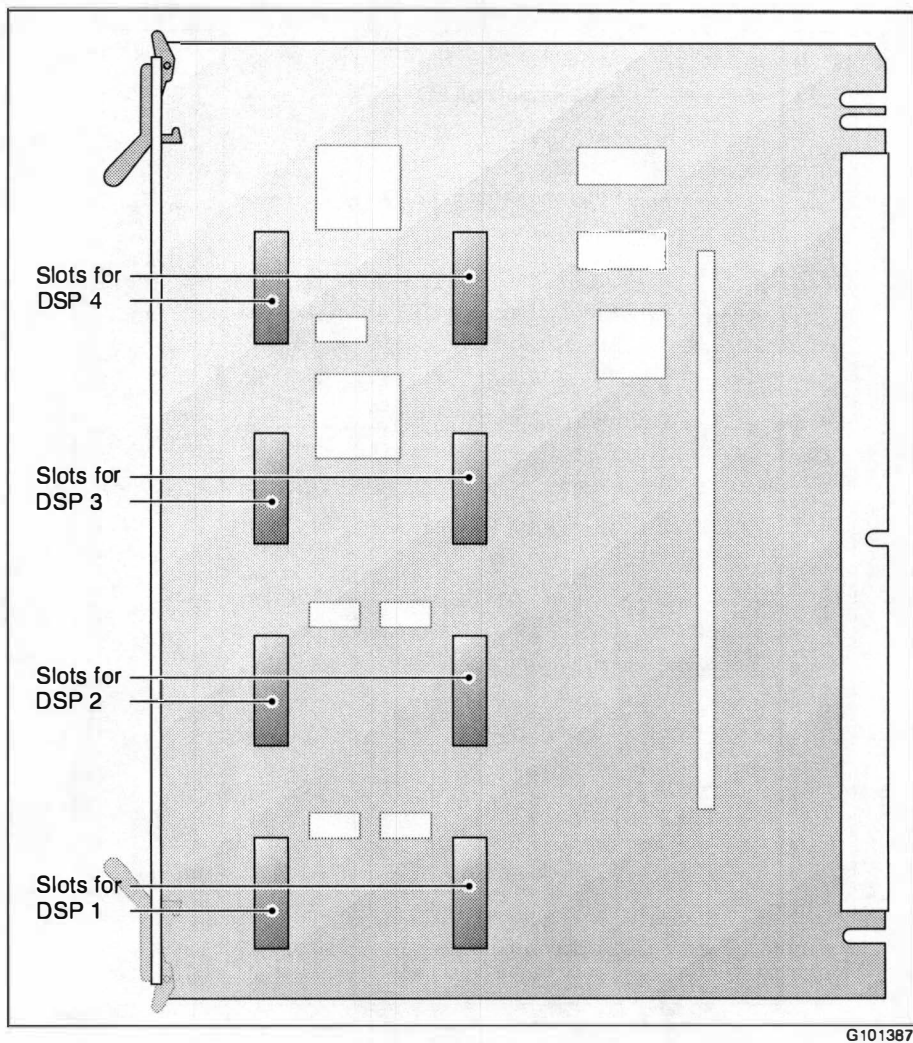
Destination	Order code
IPE shelf	NTDR70xx
Option 11 cabinet	NTDR71xx

Regardless of order code, the motherboard of the 32-port RLC is the same circuit pack that is used for the 16-port RLC. The illustration on page 5 shows the circuit pack. The RLC motherboard conforms to the Common Features Specification for IPE line cards.

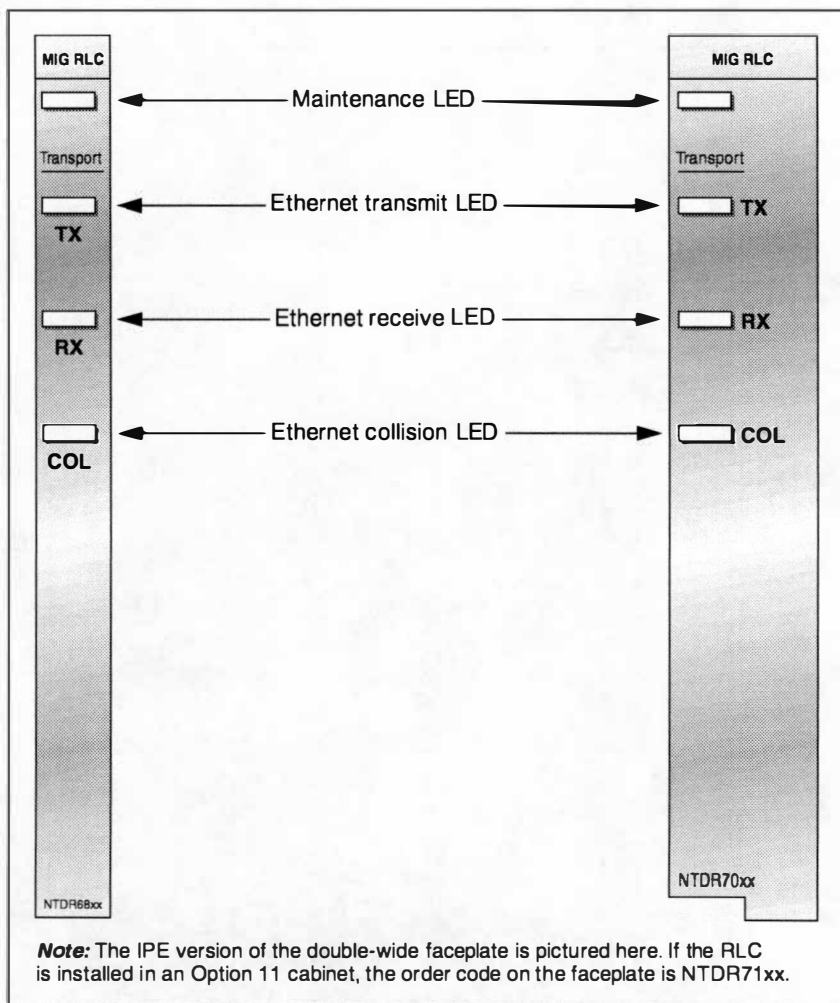
PBX software compatibility

The RLC is compatible with Meridian 1 software Release 23 or higher.

RLC motherboard



RLC faceplates: 16-port and 32-port



G101386

LED indicators

The red Maintenance LED on the faceplate indicates the basic health of the RLC, as with all other IPE line cards. Under normal conditions, the Maintenance LED lights under firmware control at power up and blinks three times after a successful self-test. This LED remains lit until the host PBX enables the RLC, then it goes out. If the host PBX disables the RLC, the Maintenance LED comes on and stays on.

Other characteristics of the Maintenance LED include:

- If the Maintenance LED comes back on after the RLC passes its self-test, ensure that the card is enabled. (Refer to the host PBX documentation for the correct procedure.) If the RLC is enabled and the Maintenance LED remains on, there is a problem at the host PBX.
- If the Maintenance LED blinks repeatedly at one-second intervals, reseal the card at the host PBX by lifting the ejector tabs outward and pulling the RLC toward yourself. This action breaks the connection between the line card and the backplane.

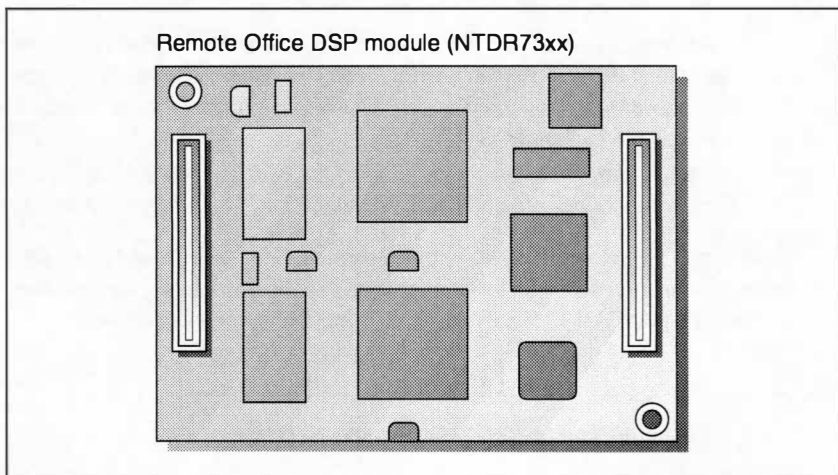
After breaking this connection, reinsert the card completely into its slot. If the RLC still does not complete a successful self-test, it must be replaced.

Three other faceplate LEDs monitor transmit activity, receive activity, and collisions on the RLC's Ethernet interface. The illustration on page 6 shows the 16- and 32-port RLC faceplates with the function of each LED labeled.

DSP application modules (NTDR73xx)

The RLC's on-board digital signal processor (DSP) resources provide voice processing for up to eight simultaneous telephone calls. Each DSP application module provides an additional eight channels of packet voice processing. To extend your system's voice processing capacity, you can add up to four DSP application modules. The illustration on page 5 shows the locations of DSP expansion slot pairings on the RLC. For help in determining the number of DSP application modules you need to increase your system's call-processing capabilities to the desired level, refer to "Installing DSP application modules" on page 72, and the RLC "System expansion worksheet" on page 293.

The following illustration shows a DSP application module. One DSP application module holds two DSP devices:



G101388

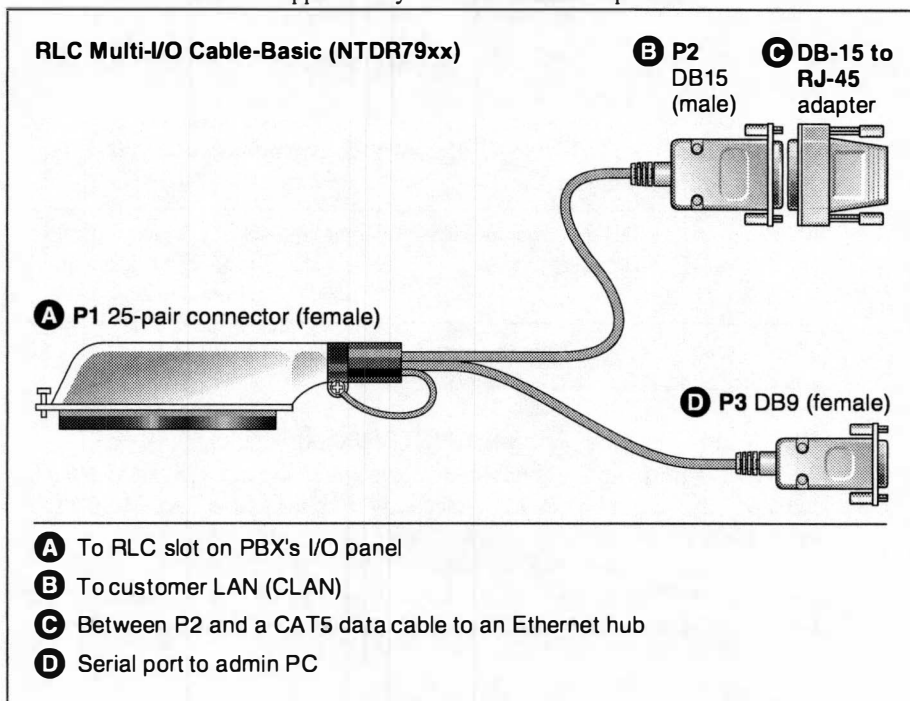
RLC cables

RLC cables connect at the I/O panel of the shelf or cabinet in the host PBX. Nortel Networks offers two cables that enable users to add the RLC to a variety of existing network configurations.

RLC Multi-I/O cable–Basic (NTDR79xx)

The Basic cable provides 10BaseT connectivity to the corporate LAN for Voice over IP (VoIP) and administration access, and RS-232 connection for serial port administration.

Note: The RLC supports only 10BaseT Ethernet speeds.



G101389

The following table describes the RLC Multi-I/O cable–Basic:

The connector labeled	is a	that transmits	and connects to the
P1	25-pair connector (female)	all signals	I/O panel.
Note: If you are using a 32-port RLC, insert P1 into the socket for the first of the two card slots occupied by the RLC.			
P2	DB-15 connector (male)	10BaseT signaling	CLAN Ethernet (customer LAN on the network).
Note: P2 requires a DB-15 to RJ-45 converter (part number 301-00001-01, shipped with the cable).			
P3	DB-9 connector (female)	RS-232 signaling	serial port to admin PC for administration and maintenance.

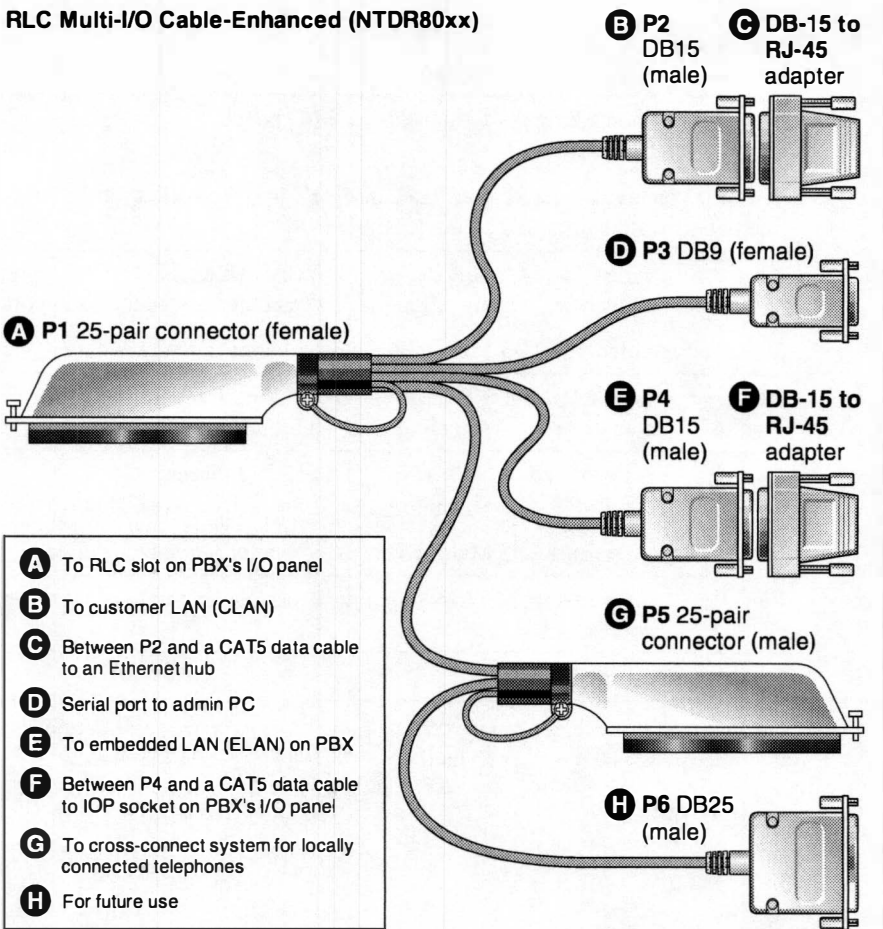
The length of this cable, from the termination end of P1 to the termination end of any other plug, is 0.6 meters (2 feet).

RLC Multi-I/O cable–Enhanced (NTDR80xx)

The RLC Multi-I/O cable–Enhanced allows you to use the RLC’s complete functionality. In addition to the connectivity supplied by the RLC Multi-I/O cable–Basic (refer to page 9), the RLC Multi-I/O cable–Enhanced adds connectivity to the host PBX’s internal (or embedded) Ethernet for switch maintenance. With the Enhanced cable you can also service locally connected telephones through RLC ports not used for remote service purposes.

Note: The RLC supports only 10BaseT Ethernet speeds.

RLC Multi-I/O Cable-Enhanced (NTDR80xx)



G101390

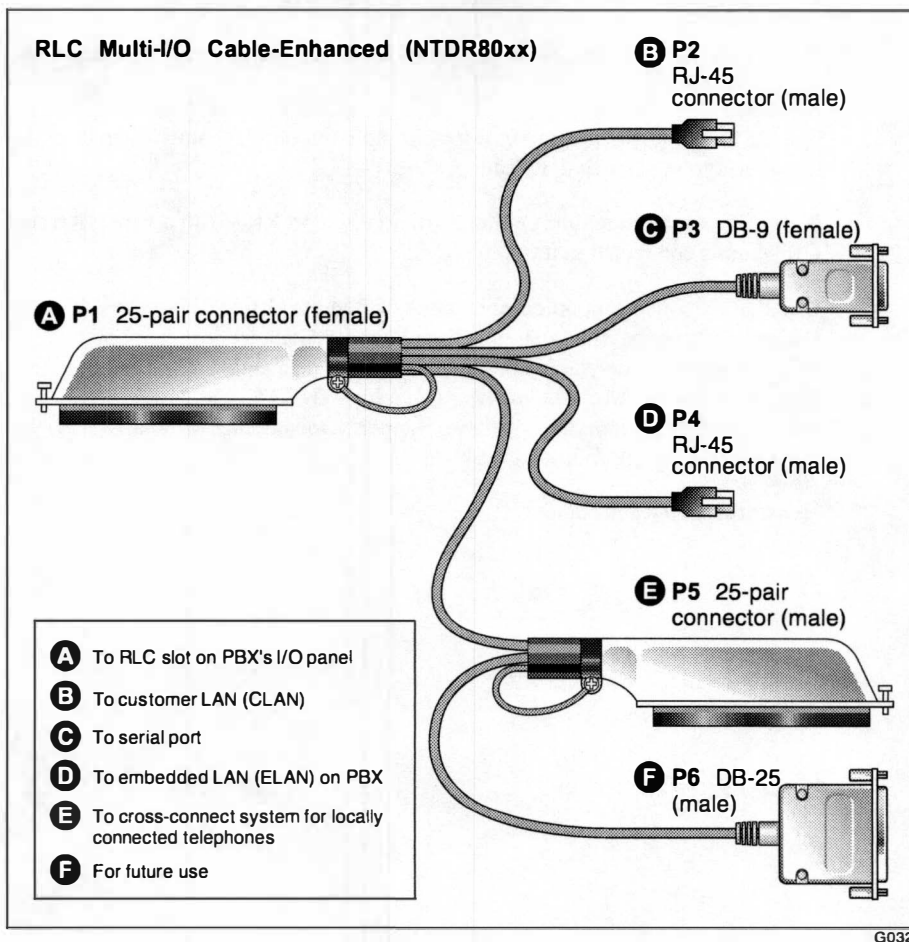
The following table describes the RLC Multi-I/O cable–Enhanced:

The connector labeled	is a	that transmits	and connects to the
P1	female 25-pair connector	all signals	I/O panel.
Note: If you are using a 32-port RLC, insert P1 into the socket for the first of the two card slots occupied by the RLC.			
P2	male DB-15 connector	10BaseT signaling	CLAN Ethernet (customer LAN on the network).
Note: P2 requires an RJ-45 Male to Female converter (already installed).			
P3	female DB-9 connector	RS-232 signaling	serial port to admin PC for administration and maintenance.
P4	male DB-15 connector	10BaseT signaling	ELAN Ethernet (host PBX's embedded LAN).
Note: P4 requires an RJ-45 Male to Female converter (already installed).			
P5	male 25-pair connector	TCM signaling	cross-connect to local telephones.
P6 is reserved for future use.			

The length of this cable, from the termination end of P1 to the termination end of any other plug, is 0.6 meters (2 feet).

Installations outside North America

RLC installations outside North America that use the RLC Multi-I/O cable-Enhanced require the cable shown in the following illustration:



Remote unit capacity on RLCs

One RLC supports a maximum of 20 Remote Office 911x series units or Meridian Digital Telephone Internal or External IP Adapter units.

Note: This scenario requires a 32-port RLC with no other Remote Office units connected to it.

One RLC supports a maximum of four Remote Office 9150 units when there are no other Remote Office units connected to the RLC.

Note: This scenario requires either a 16- or a 32-port RLC with no other Remote Office units connected to it.

One RLC can also support combinations of Remote Office 911x series, Remote Office 9150, and Meridian Digital Telephone IP Adapters. To learn about the conditions that allow you to combine these units on a single RLC, refer to the *Remote Office Network Engineering Guidelines* (NTP 555-8421-103). To locate this document, click on the Customer Support, Documentation, and North America links at the following website:

www.nortelnetworks.com

Operational characteristics

The RLC provides a number of unique features that distinguish it from other remote service products.

These features include:

- adjustable quality of service using QoS Transitioning Technology
- port sharing options
- multiple security levels
- packet voice processing
- dial-up trunking
- bandwidth allocation
- Meridian telephone equipment compatibility

Adjustable quality of service using QoS Transitioning Technology

Nortel Networks' patented QoS Transitioning Technology monitors the quality of service (QoS) level on the internet protocol (IP) portions of your Remote Office system. This feature detects poor voice QoS when it occurs. The QoS level is a user-oriented metric that takes one of ten settings. Using Configuration Manager, you can select an acceptable transition threshold from among the ten predefined settings to identify the limits of acceptable voice QoS.

Configuring QoS Transitioning Technology to provide satisfactory results requires a detailed understanding of traffic on your IP network. For guidance on evaluating and adjusting your network's QoS, refer to the *Remote Office Network Engineering Guidelines* (NTP 555-8421-103). Refer to page 14 for instructions on obtaining this document.

Quality of service on shared networks

High volumes of data packets can cause QoS problems for voice traffic on shared networks. Configuring the router to send voice packets ahead of data packets (prioritizing voice packets) can address some QoS concerns. For further details, refer to "Prioritizing voice traffic over shared networks" on page 161.

Port sharing options

The RLC allows you to take maximum advantage of your host PBX's port resources regardless of what time it is or who is working. Dynamic port pooling and multi-user ports allow more than one person or station to use the same port on the host PBX. Dynamic port pooling and multi-user ports allow for more flexible, less restrictive use of the corporate telecommunications network.

Dynamic port pooling

Dynamic port pooling allows multiple users or stations to time-share the same port on the host PBX. No correlation exists between a user or station and the TN or DN on the host PBX when no one is registered.

When users share ports in a dynamic pool register, they receive the next available port in the pool regardless of that port's TN or DN. Users register by entering the Registration SPRE (Special Prefix) code on their telephone keypad. Refer to the Installation and Administration Guide for your specific Remote Office unit for details.

Note: If there are no available ports in the pool when a user tries to register, that user hears a fast busy signal.

When users press the primary DN key on their digital telephone set to place an outgoing call, they receive the DN assigned to them at registration. While registered, users also receive all calls placed to that DN. When users are ready to release their ports on the host PBX, they enter the deregistration SPRE code. This allows registering users to access that port.

Multi-user ports

Like dynamic port pooling, multi-user ports also allow multiple users or stations to time-share ports on the host PBX. With a multi-user port, however, there is a specific correlation between the user or physical station and the TN or DN on the host PBX. The host PBX blocks users configured to a multi-user port from accessing that port if another configured user is currently registered to the port. Multi-user ports are available only to users specifically configured to the ports.

While multiple users in a dynamic port pool can be active at the same time, only one user can be active on a multi-user port.

You can configure a multi-user port to allow one user to access the same port from multiple locations. This feature can give one person access the same port from both the corporate office and the home office. Refer to the Installation and Administration Guide for your specific Remote Office unit for details.

Multiple security levels

The RLC allows you to choose from three levels of protection from unauthorized access to your host PBX through the Remote Office system. Select one of the following security levels to regulate usage of corporate telecommunications resources:

- Level 1, no security

When you set RLC security to security level 1, the RLC allows all calls to route through the host PBX, regardless of source.

Note: Level 1 is the RLC's default security level.

- Level 2, caller ID security

When you set RLC security to security level 2, the RLC does the following:

- a. It compares the caller ID of the incoming call against the caller IDs configured for this remote unit.
- b. It denies PBX access to this call if the caller ID does not match any of those in this unit's List of Caller IDs.

For the required steps to configure security level 2 on your RLC, refer to "Remote Connection Configuration" on page 171.

Note: Level 2 security is not applicable when using Remote Office 911x series units with the RLC.

- Level 3, provisioned security

When security is set to level 3, depending on the unit that initiated the call, the following call verification occurs:

- a. If a remote unit calls the RLC, the RLC compares its Inbound security ID with this remote unit's Outbound security ID. If they match, the RLC accepts the call, otherwise, it rejects the call.
- b. If the RLC calls a remote unit, the remote unit compares its Inbound security ID with the RLC's Outbound security ID. If they match, the remote unit accepts the call, otherwise, it rejects the call.

For the steps required to configure security level 3 on your RLC, refer to “Remote Connection Configuration” on page 171.

Security configuration applies to all ports of a Remote Office unit. That is, all ports on one Remote Office 9150 unit have the protection of the same security level.

Packet voice processing

All connections to the host PBX support the following features:

Voice compression

The RLC supports G.711, G.726, and G.729A voice compression standards. You can configure different ports with different voice compression algorithms. This feature allows you to configure different voice QoS for different users.

Note: Remote Office 911x units only support G.729A compression in Public Switched Telephone (PSTN) mode. They support G.711 and G.729A in VoIP mode.

Voice jitter attenuation buffer

The RLC’s dynamic voice jitter attenuation buffer compensates for the uneven arrival of voice packets at their destinations over a given period of time across data networks. This buffer collects packets that arrive unevenly and relays them evenly.

Packet-loss handling techniques

The RLC uses packet-loss handling techniques to accommodate missing packets or packets that arrive too late to be processed into the real-time voice stream.

Silence suppression algorithm

To save bandwidth, a silence suppression algorithm prevents packet transmission during periods when Voice Activity Detection (VAD) determines that there is no voice data present. The receiving end inserts comfort noise to assure the user that the line is still active.

Echo cancellation

The RLC performs echo cancellation in accordance with ITU G.168, and cancels echo with a tail length of up to 32 milliseconds (32 ms).

Dial-up trunking

The RLC supports digital trunks for connections to the Remote Office units. The RLC shares the host PBX's digital trunks (ISDN PRI) for a PSTN connection to the Remote Office unit.

QoS Transitioning Technology

The RLC supports PSTN interfaces for local calling when used in Voice over IP (VoIP) mode. In this way, it also supports QoS Transitioning Technology.

For a further explanation of QoS transition functions, refer to "Adjustable quality of service using QoS Transitioning Technology" on page 15. For exact configuration procedures, refer to "Configuring Quality of Service" on page 182.

Bandwidth utilization

The voice compression algorithm that you choose when configuring DSP resources determines the bandwidth utilization of the RLC. The RLC currently supports the following compression algorithms with the Remote Office devices indicated in the table below:

The compression algorithm	uses a compressed bit rate of	on the following Remote Office devices:
G.711	64 Kbps	9150
G.726	32 Kbps	9150
G.729A	8 Kbps	911x, 9150, Meridian Digital Telephone IP Adapter

Dynamic trunk bandwidth allocation

In PSTN mode, the RLC dynamically allocates available trunk bandwidth to maximize bandwidth use. That is, as the RLC initiates calls and bandwidth requirements increase, the RLC establishes additional trunk connections for Remote Office 9150 units.

Call on-demand

The RLC supports full call on-demand (COD) functionality. This includes minimum call duration and idle timers that you can configure according to your service provider's fee structure. COD refers to the way that the RLC handles host trunk connections. In the COD mode of operation, the RLC does not establish a host connection until the user places a call to a host DN. The COD connection stays active until the minimum call duration timer expires. The RLC then closes the host connection, if idle. If another user initiates a call to the host before the timer expires, the RLC resets the timer to track the last call established. There is a single timer for each Remote Office 9150 or 911x unit.

Timers

The RLC has two timers to help manage PSTN costs.

- **Minimum call duration timer**

Most PSTN tariffs specify the minimum length of time that providers can charge users for opening a connection, regardless of the call duration. This length of time determines the minimum call charges listed on long-distance telephone bills.

Remote Office 9110, 9115, and 9150 units use the minimum call duration timer in PSTN mode only. This timer specifies the minimum length of time that each PSTN call to the host PBX remains open, regardless of telephone activity. You can configure the timer on the RLC to drop the connection just before the beginning of the next charge period, when the cost of the call increases. (Refer to Example 1 on page 21.)

- **Idle timer**

Remote Office 9110, 9115, and 9150 units also use the idle timer in PSTN mode only. This timer identifies the maximum length of time a PSTN connection must remain idle before the RLC closes the connection.

An idle connection exists when no voice connections (voice paths) remain open and when no data paths exist. Users at the remote site create data paths when they press keys on their digital telephones. Signaling passing from the host PBX to the digital telephone also creates data paths.

If anyone at the remote site places another call within 60 seconds, the RLC resets the idle timer and uses the existing PSTN connection for the new call. This eliminates the need to open a new PSTN connection and incur unnecessary long distance charges. (Refer to Example 2 on page 21.)

The minimum call duration and idle timers work together to control PSTN long distance charges. The following examples describe what happens when the minimum call duration timer is set to 59 seconds and the idle timer is set to 60 seconds.

Example 1

After a 20-second call, the minimum call duration timer still has 39 seconds remaining. If no one else at the remote site places a call, the RLC drops the PSTN connection when the timer reaches 59 seconds. In this example, the minimum call duration timer expires before the RLC initiates the idle timer.

- After the minimum call timer, PSTN signaling with no digital telephone activity keeps the primary PSTN connection up for no longer than two idle timers.
- Every PSTN connection remains active for at least the length of the minimum call timer.
- Additional trunks and circuit-only trunks active longer than the minimum call timer remain active for an additional idle timer duration. This is the case only if no additional bandwidth requests come to the host PBX.

Example 2

After a 65-second call, the idle timer starts. If no one at the remote site places a call during the next 60 seconds, the RLC drops the PSTN connection. Since the PSTN call exceeds 59 seconds, the minimum call duration timer expires before activity ceased. At the conclusion of the call, the RLC initiates the idle timer to prevent unnecessary charges.

DN priority

The RLC provides multiple priority levels for Remote Office 9150 unit users:

- PSTN only
- high
- normal
- IP only

If you configure this feature, you must also configure an amount of bandwidth to save for the High priority DNs. You must also identify the privileged DNs through Configuration Manager. This information does not apply to Remote Office 911x series or Meridian Digital Telephone IP Adapters.

The RLC uses the *priority reserved* bandwidth for high priority DNs. When only bandwidth for *high* priority DNs remains on the network, users dialing out on *normal* priority DNs hear a fast busy signal. For details on configuring DN priority, refer to “RLC port configuration” on page 162.

Online/Offline table

You can configure the RLC to establish or terminate host connections at specified times of the day. This feature limits excessive connection charges for idle host connections. For details on configuring the Online/Offline table, refer to “Online/Offline table configuration” on page 189.

Bandwidth allocation

Configuration Manager provides options for you to allocate PSTN bandwidth for Remote Office 9150 stations. This does not apply to Remote Office 911x series or Meridian Digital Telephone IP Adapters.

- Priority reserved bandwidth

You can reserve bandwidth for certain DNs that need prioritized access to Remote Office channels. You can configure high priority DNs on the RLC Port Configuration property sheet. These DNs consume Priority Reserved Bandwidth before using unreserved bandwidth.

- Extra bandwidth

Configuration Manager allows you to reserve a certain amount of bandwidth for accessing a remote unit. When the amount of bandwidth available falls below the level that you configure, the RLC opens additional B-channels to the remote unit.

Meridian digital telephone hardware compatibility

The RLC is compatible with the following Meridian digital telephone equipment:

Models		Modules
■ M2006 ⁱ	■ M3310	■ add-on modules ⁱⁱⁱ
■ M2008D	■ M3820	■ key-expansion modules
■ M2008HFD	■ M3901 ^{i, ii}	
■ M2216D	■ M3902	
■ M2616D	■ M3903	
■ M2616CT	■ M3904	
■ M3110 ⁱ	■ M3905	

- i. Remote Office 911x units and Meridian Digital Telephone IP Adapters do not support M2006, M3110, or M3901 telephones.
- ii. On the host PBX, you must configure M3901 telephones as M3902 telephones for proper operation with Remote Office 911x units or Meridian Digital Telephone IP Adapters
- iii. Add-on modules include key based add-on modules (KBAs) and display-based add-on modules (DBAs) for M39xx sets.

Footstand

Installation of a Remote Office 9110 unit or a Meridian Digital Telephone Internal IP Adapter unit requires an ATA/MCA footstand. Meridian Modular Telephones (M2000 series) with a date code of May 6, 1998 or later come equipped with the required footstand. Contact your Nortel Networks distributor to obtain the necessary footstand if your telephone has an earlier date code.

Data channel adapters

The Remote Office 9150 unit supports the following types of data channel adapters:

- Analog Telephone Adapters (ATAs)
Note: The Remote Office systems using ATAs do not support modems.
- Meridian Communication Adapters (MCAs)

Note: MCAs use the secondary data channel of the TCM telephone interface and require a full 64 Kbps of bandwidth. If you have a 56 Kbps connection, ensure that this connection provides multiple B-channels. Refer to “Understanding port relationships” on page 105 for information about port assignment for data channel adapters.

A 16-port RLC handles up to four data channel adapters. A 32-port RLC handles up to seven data channel adapters.

Note: Remote Office 911x units and Meridian Digital Telephone IP Adapters do not support data channel adapters.

Nortel Networks CTI and ACD applications

The RLC operates with all Nortel Networks computer telephony interface (CTI) and automatic call distribution (ACD) applications.

How the RLC works

When a call comes through the host PBX to a user at a remote location, the RLC makes a connection to the appropriate remote unit. The host PBX completes the call. If the RLC cannot establish a connection, the call rings until the host PBX forwards it to voice-mail.

Initiate outgoing calls by either picking up your telephone's handset or pressing a line appearance key. There are two types of appearance keys:

- host call appearance keys, used to place calls to the host site
- local call appearance keys, used to place calls to another station at the branch office, or to place and receive calls through the local PSTN

Details of the outgoing call process appear in the diagrams and procedures on pages 27–31.

RLC processing modes

The RLC processes calls for a Remote Office network in one of two modes:

- host-controlled
- locally controlled

Host-controlled calls

When you place a call to someone at your host site, or when someone at your host site calls you, the call is processed in host-controlled mode. The RLC routes such calls through the host PBX. Details of host-controlled call processing for the Remote Office 9150 unit appear in the diagrams and procedures on pages 27–30.

Locally controlled calls

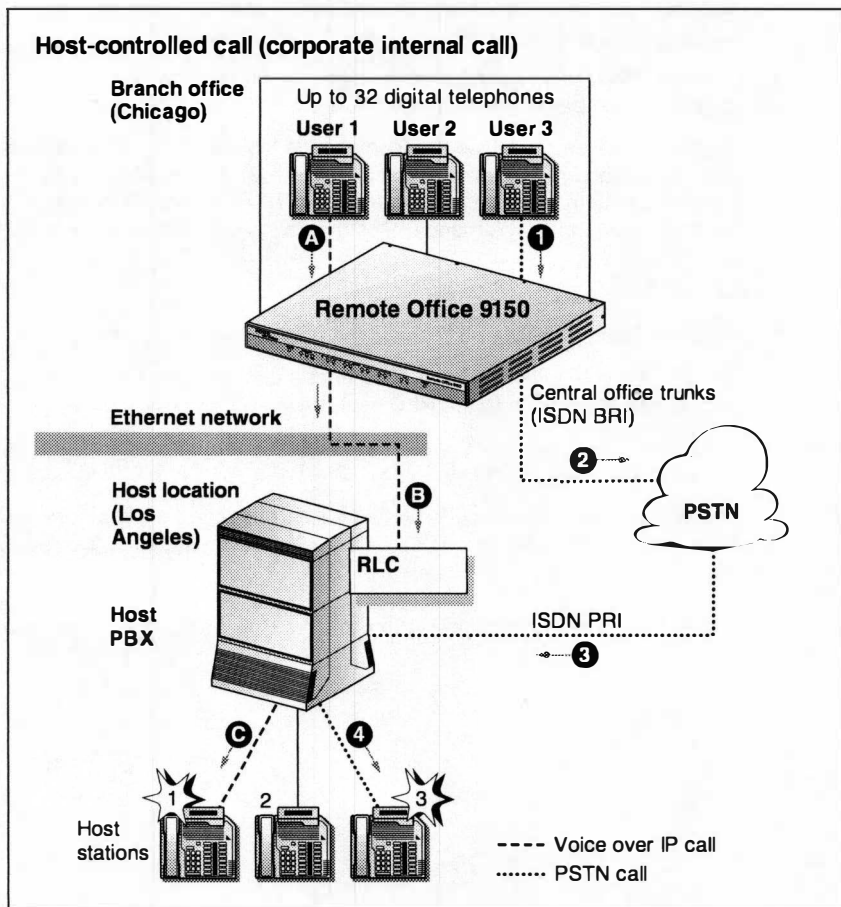
There are three types of locally controlled calls:

- A Remote Office 9150 unit user begins a call by pressing one of the local calling keys. The user then dials the DN of another local calling key. The Remote Office 9150 unit processes this call.
- A Remote Office 9150 unit user begins a call by pressing one of the local calling keys. The user then dials a local trunk access code. The local PSTN processes this call. Refer to the diagram on page 31.
- A Remote Office 911 x series user begins a call by pressing a key configured as a local calling key. The user then dials a local telephone number. The local PSTN processes this call. Refer to the diagram on page 37.

The host PBX is not involved in any of the call scenarios above. These scenarios describe calls processed in the locally controlled mode.

9150 call scenario 1: Host-controlled mode—internal corporate call

The following diagram shows how the Remote Office system routes a host-controlled call from a Remote Office 9150 unit to the corporate office.



G101392

The network that routes the host-controlled call is transparent to the user. Both VoIP and PSTN calls present the same dialing requirement, as described on page 28.

Voice over IP network call

- 1 Remote Office 9150 user 1 presses the host call appearance key (item A).
Result: Remote Office 9150 user 1 hears a dial tone. This indicates a successful connection to the RLC over the IP network.
- 2 Remote Office 9150 user 1 dials a telephone number (such as the extension number of host station 1).

Result: The Remote Office 9150 unit sends the dialed digits as packets across the Ethernet network to the RLC (item B). The RLC converts the packets to the format required by the host PBX. The host PBX then converts the data to voice and routes the call to host station 1 (item C).

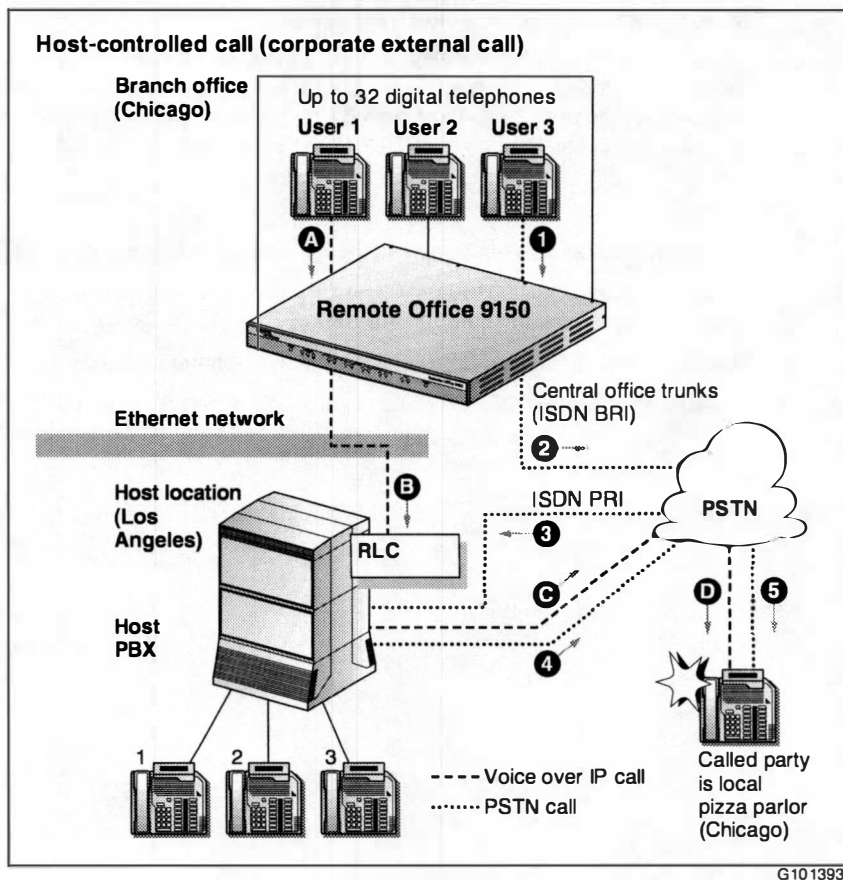
PSTN call

- 1 Remote Office 9150 user 3 presses the host call appearance key (item 1).
Result: Remote Office 9150 user 3 hears a dial tone. This indicates a successful connection to the RLC over the PSTN.
- 2 Remote Office 9150 user 3 dials the telephone number, such as the extension number of host station 3.
Result: The Remote Office 9150 unit sends the dialed digits across ISDN BRI through the PSTN, through the host PBX to host station 3 (items 2, 3, & 4).

Note: Item notations in parentheses refer to circled markers in the diagram on page 27.

9150 call scenario 2: Host-controlled mode—external corporate call

The following diagram also shows how a Remote Office system routes a host-controlled call from a Remote Office 9150 unit. In 9150 call scenario 2, the call routes to a party outside the organization.



The network that routes the host-controlled call is transparent to the user. Both VoIP and PSTN calls present the same dialing requirement, as described on page 30.

Voice over IP network call

- 1 Remote Office 9150 user 1 presses the host call appearance key (item A).

Result: Remote Office 9150 user 1 hears a dial tone. This indicates a successful connection to the RLC over the IP network (item B).

- 2 Remote Office 9150 user 1 dials the external telephone number.

Result: The Remote Office 9150 unit sends the dialed digits as packets across the Ethernet network. The RLC converts the packets to the format required by the host PBX. The host PBX then converts the data to voice and routes the call through the PSTN to the called party (items C & D).

PSTN call

- 1 Remote Office 9150 user 3 presses the host call appearance key (item 1).

Result: Remote Office 9150 user 3 hears a dial tone. This indicates a successful connection to the RLC over the PSTN (items 2 & 3).

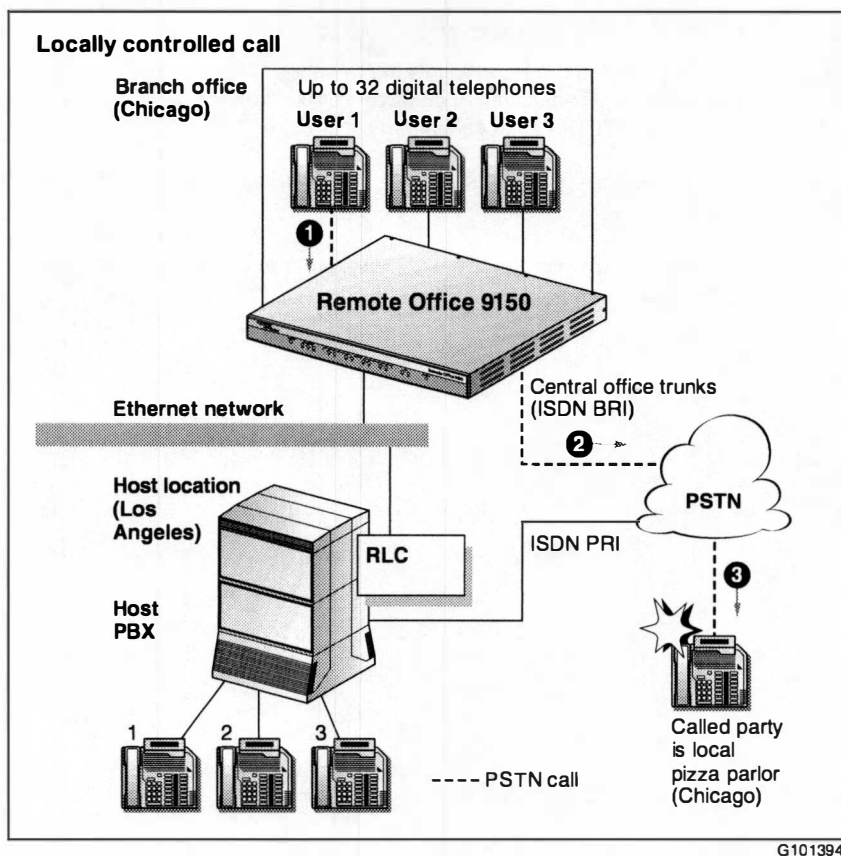
- 2 Remote Office 9150 user 3 dials the external telephone number.

Result: The Remote Office 9150 unit sends the dialed digits across ISDN BRI through the PSTN, through the host PBX to the called party (items 4 & 5).

Note: Item notations in parentheses refer to circled markers in the diagram on page 29.

9150 call scenario 3: Locally controlled mode—local call

The following diagram shows how a Remote Office system routes a call within your local area.



Local call

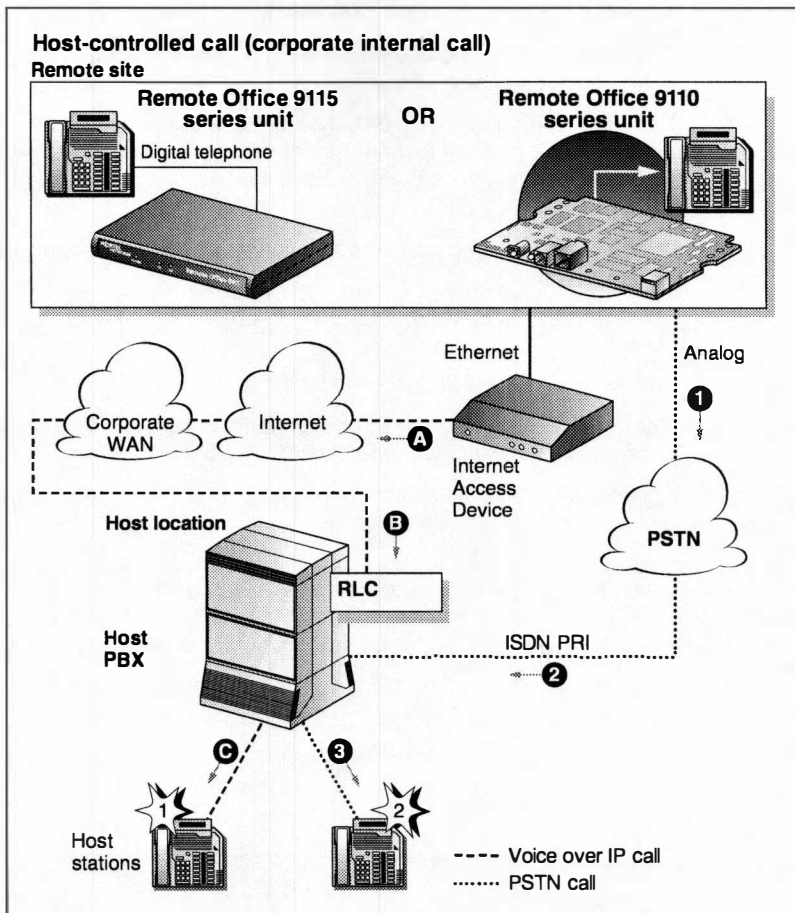
- 1 Remote Office 9150 User 1 presses the local call appearance key and hears a dial tone from the Remote Office 9150 unit (item 1).
- 2 Remote Office 9150 User 1 then dials a trunk access code and hears a PSTN dial tone from the Central Office (item 2).
- 3 Remote Office 9150 User 1 dials the telephone number (the pizza parlor in this example). The dialed digits travel across the ISDN BRI connection through the PSTN to the called party (item 3).

Note: Item notations in parentheses refer to circled markers in the diagram on page 31.

For details about how the Remote Office system routes calls from Remote Office 911x series units, refer to pages 33 through 37.

911x call scenario 1: host-controlled—corporate internal call

The following diagram shows how the Remote Office system routes a host-controlled call from a Remote Office 911x unit to the corporate office.



G019

The network that routes the host-controlled call is transparent to the user. Both VoIP and PSTN calls present the same dialing requirement, as described on page 34.

Voice over IP network call

- 1 The Remote Office 911x user lifts the handset (item A).
Result: The Remote Office 911x user hears a dial tone. This indicates a successful connection to the RLC over the IP network (item B).
- 2 The Remote Office 911x user dials a telephone number, such as the extension number of host station 1.
Result: The Remote Office 911x unit sends the dialed digits as packets through the IP network to the Ethernet network or Corporate WAN to the RLC. The RLC converts the packets to the format required by the host PBX.
- 3 The host PBX then converts the data to voice and routes the call to host station 1 (item C).

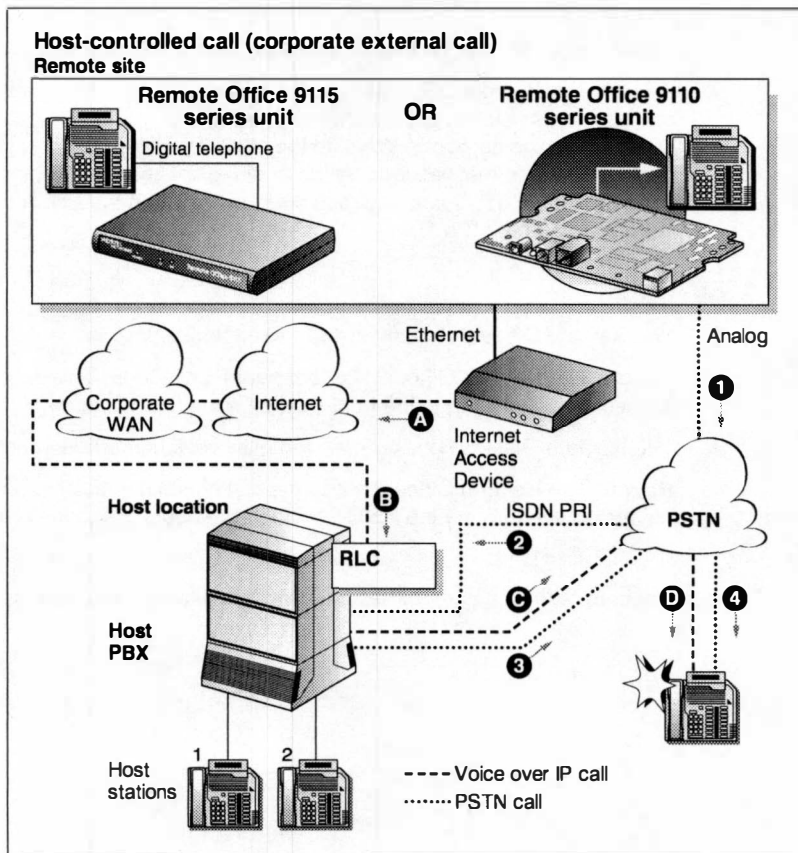
PSTN call

- 1 The Remote Office 911x user lifts the handset.
Result: The Remote Office 911x user hears a dial tone. This indicates a successful connection to the RLC over the PSTN (item 1).
- 2 The Remote Office 911x user dials a telephone number, such as the extension number of host station 2.
Result: The Remote Office 911x unit sends the dialed digits across the PSTN through the host PBX (item 2) to host station 2 (item 3).

Note: Item notations in parentheses refer to circled markers in the diagram on page 33.

911x call scenario 2: host-controlled—corporate external call

The following diagram also shows how a Remote Office system routes a host-controlled call from a Remote Office 911x series unit. In 911x call scenario 2, the call routes to a party outside the organization.



G020

The network that routes the host-controlled call is transparent to the user. Both VoIP and PSTN calls present the same dialing requirement, as described on page 36.

Voice over IP network call

- 1 The Remote Office 911x user lifts the handset (item A).

Result: The Remote Office 911x user hears a dial tone. This indicates a successful connection to the RLC over the IP network and the corporate WAN (item B).

- 2 The Remote Office 911x user dials the external telephone number.

Result: The Remote Office 911x series unit sends the dialed digits as packets across the Ethernet network. The packets go through the IP network and the corporate WAN, to the RLC. The RLC converts the packets to the format required by the host PBX. The host PBX then converts the data to voice and routes the call through the PSTN to the called party (items C & D).

PSTN call

- 1 The Remote Office 911x user lifts the handset (item 1).

Result: The Remote Office 911x user hears a dial tone. This indicates a successful connection to the host PBX over the PSTN (item 2).

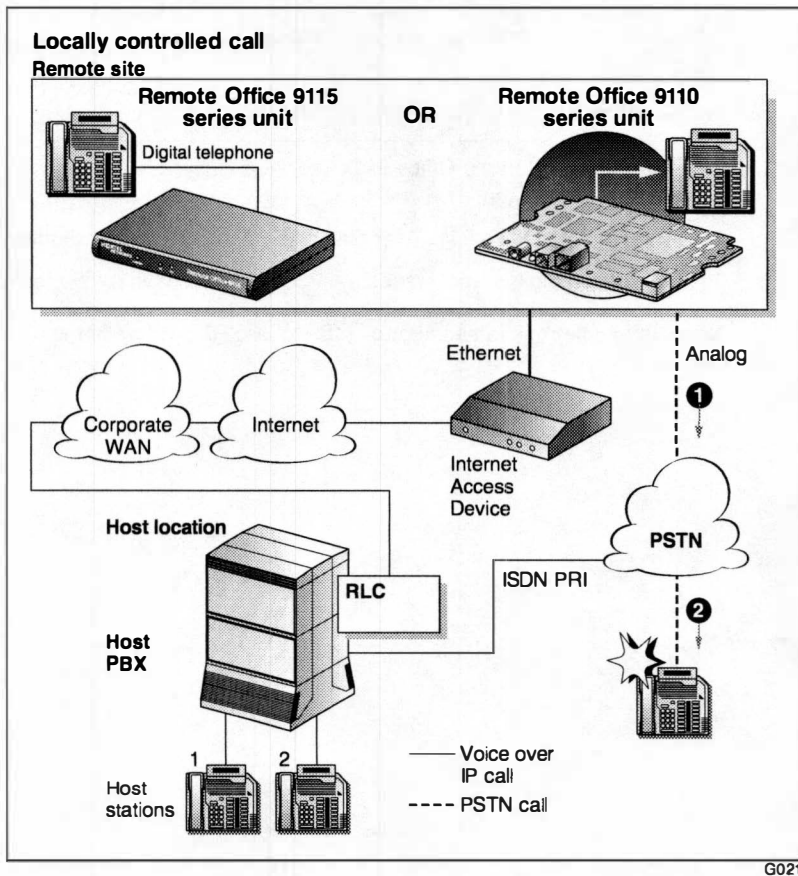
- 2 The Remote Office 911x user dials the external telephone number.

Result: The Remote Office 911x series unit sends the dialed digits across an analog line through the PSTN, through the host PBX to the called party (items 3 & 4).

Note: Item notations in parentheses refer to circled markers in the diagram on page 35.

911x call scenario 3: locally controlled mode—local call

The diagram below shows how a call is routed when placing a call within your local area using a Remote Office 911x series unit.



Local call**1**

IF the Remote Office 911x unit is **THEN the Remote Office 911x user**

offline, or not connected to the host PBX, lifts the handset.

online, or connected to the host PBX, presses the local calling key

Result: The Remote Office 911x user hears a PSTN dial tone from the Central Office (item 1).

- 2** The Remote Office 911x user dials the external telephone number.
- 3** The dialed digits travel across the PSTN to the called party (item 2).

Note: Item notations in parentheses refer to circled markers in the diagram on page 37.

Environmental requirements

The RLC withstands the following environmental conditions without any performance degradation or damage.

Note: In this section, the phrase *short term* means 72 consecutive hours with a maximum of 360 hours per year. The temperature ratings are for the environment of the circuit and not the total system.

Operating temperature

Normal	+10 to 45 °C
Short Term	0 to +55 °C

Operating humidity

Normal	10% to 95% (noncondensing)
Short Term	5% to 95% (noncondensing)

Storage

Temperature	-50 to +70 °C
Humidity	5% to 95% RH (noncondensing)

Power requirements

This section lists characteristics of the recommended power supplies for the Remote Office 9150 unit, the Remote Office 911x series units, and the Meridian Digital Telephone IP Adapter units.

9150 units

Input specifications for the Remote Office 9150 unit are as follows:

Characteristics	Rating
voltage	85 - 264 VAC
frequency	47 - 63 Hz
current	3.20A maximum, 115 VAC (North American installations) 1.80A maximum 230 VAC (non-North American installations)

Output specifications for the Remote Office 9150 unit are as follows:

Characteristic	Rating
Output 1 voltage	5VDC +/-5%
Output 1 current	10.0A maximum
Output 2 voltage	24VDC +/-5%
Output 2 current	3.0A maximum
maximum power	110W

Remote Office 911x series and Meridian Digital Telephone IP Adapter units

Input specifications for the Remote Office 911x series units, including the Meridian Digital Telephone IP Adapter units, are as follows:

Characteristic	Rating
voltage	90 - 264 VAC
frequency	47 - 63 Hz
current	0.4A maximum

Output specifications for the Remote Office 911x series units, including the Meridian Digital Telephone IP Adapter units, are as follows:

Characteristic	Rating
voltage	24 VDC +/-5%
current	0.62A maximum
power	15W maximum

Chapter 2

Planning for RLC installation

In this chapter

Preinstallation preparation	44
RLC Installation Checklist	48
System resources management	54
Network considerations	58
Administration PC	60
Planning for future growth	64
Deployment options	65

Preinstallation preparation

To prepare a site for installation, consider the environment, structural and electrical factors, and other site-specific limitations. For more information on site-preparation from an equipment standpoint, refer to the following documents:

- *Meridian 1 Installation and Planning* (NTP 553-3001-120)
- *Meridian 1 System Engineering* (NTP 553-3001-151)
- *Meridian 1 Power Engineering* (NTP 553-3001-152)
- *Meridian SL-100 Intelligent Peripheral Equipment-IPE* (NTP 555-4001-129)
- *Succession Communication Server for Enterprise 1000 Planning and Installation Guide* (NTP 553-3023-210)

Planning for your remote service needs

Plan for your remote service needs by determining the total number of simultaneous remote service telephone calls you want to support on your network. This number tells you how many RLC ports that you need.

RLC requirements

Once you have determined the total number of RLC ports that you need in your remote service network, you can determine the number and size of RLCs needed at your host site.

Every 16 remote service ports in your network requires one card slot in the host PBX and 16 ports on an RLC. If you want your network to support more than 16 remote service ports, you need at least one 32-port RLC.

The following table gives a summary of how to choose the correct size RLC for your specific remote service needs.

IF the number of remote-service ports in your network is	THEN you need
under 17,	a 16-port RLC.
between 17 and 32,	a 32-port RLC.
over 32,	to consult with your Nortel Networks distributor to determine the most cost-effective combination of 16- and 32-port RLCs.

DSP requirements

The total number of simultaneous telephone calls that you want to support also determines the number of DSP application modules that you need.

- Both 16- and 32-port RLCs come equipped with enough built-in DSP resources to provide non-blocking service for up to 8 simultaneous calls.
- Each remote telephone call to the host PBX requires one DSP channel.
- Each DSP application module has eight channels that provide eight additional voice paths between host and remote sites.

The following sample configurations illustrate the capacities of a few common RLC–DSP combinations:

1. The basic 16-port RLC ships with eight built-in DSP channels. With no hardware changes, the 16-port RLC supports up to 16 users, allowing up to eight simultaneous calls.
2. When you add one DSP application module to the 16-port RLC, the line card now holds 16 DSP channels. This combination supports up to 16 users, allowing up to 16 simultaneous calls.
3. The basic 32-port RLC ships with eight built-in DSP channels. With no hardware changes, the 32-port RLC supports up to 32 users, allowing up to eight simultaneous calls.
4. When you add three DSP application modules to the 32-port RLC, the line card has 32 DSP channels. This combination supports up to 32 users, allowing up to 32 simultaneous calls.

Note: When you add data channel adapters (MCAs and ATAs) to a remote site, that site's DSP channel usage increases. Every remote call, whether from a telephone, MCA, or ATA, requires a DSP channel.

Each DSP device configured with the 911x DSP load supports up to four modem channels.

Installation planning

Make an outline of cable routing between the I/O panel of the shelf where the RLC resides and the following components of your Remote Office system:

- your PBX's serial port
- the I/O-panel connection to the IOP (input-output port) card for access to your PBX's internal Ethernet, or ELAN
- the cross-connect device to the local telephones using the RLC ports not providing remote services

Note: The RLC operates properly without the last two connections listed above. These two connections are available only with the RLC Multi-I/O cable—Enhanced. Refer to page 10 for more information on this cable.

Deployment planning

Include the configuration settings for each station at each remote site and for each port at the host site in your deployment plan. Use Appendix A, "Planning forms", on page 275 to help with this task.

Before you can configure the system with Configuration Manager, you must configure PBX voice and data ports for each RLC port. See "Configuring remote and network ports" on page 106.

Checklists

Use the RLC Installation Checklist on page 48 as a guide to ensure complete RLC installation and configuration.

Planning forms

Appendix A, “Planning forms”, contains the following forms for you to record and store your configuration plans:

- Reach Line Card
- Connection Information—32 ports
- Online/Offline Table Configuration
- System expansion worksheet

Refer to “Related information products” on page xxii for information on accessing these forms online.

Taking inventory

After you unpack and visually inspect the equipment, verify that you have all the equipment at the site before beginning installation. Check the equipment you received against the shipping documents. Report any shortages to your Nortel Networks customer support representative immediately.

Installation checklist

When you are preparing to install your Meridian system, use the checklist on following pages to ensure that you complete all the required processes properly.

RLC Installation Checklist

Page 1 of 6

Use this checklist to ensure completion of all installation tasks.

Check	Task	For details, refer to
1. Planning		
☐	Check the Remote Office web site for the latest Release Notes with last-minute product updates.	the <i>Remote Office and RLC Release Notes</i> (NTP 555-8421-102) at the following address: www.nortelnetworks.com
☐	Ensure that you have the latest firmware and software.	the <i>Remote Office and RLC Release Notes</i> (NTP 555-8421-102). This document ships with Remote Office equipment. You can obtain additional copies online at the following address: www.nortelnetworks.com
☐	Ensure that your PBX platform and software release support the RLC.	"PBX hardware and software compatibility".
☐	Ensure that a slot is available on the PBX IPE shelf or Option 11 cabinet for each RLC. Order additional shelves if necessary.	your Nortel Networks distributor.
☐	To route calls over the IP network, the PSTN, or both, determine what you must do to implement these call routing methods.	"Deployment options".

RLC Installation Checklist

Page 2 of 6

Check	Task	For details, refer to
☐	If you want to use the IP network to route calls, evaluate the IP network to determine if the network infrastructure can support voice traffic.	■ your data network administrator ■ the <i>Remote Office Network Engineering Guidelines</i> (NTP 555-8421-103) You can obtain this document online at the following address: www.nortelnetworks.com
☐	Plan the installation and cabling of RLCs.	Chapter 2, "Planning for installation".
☐	Decide on the administration PC setup.	"Administration PC".
☐	Obtain the cables that you need to establish the needed connections to the network.	"Reach Line Card cables".
☐	Gather the configuration information (network addresses, connection numbers, online/offline schedule, QoS thresholds, and so on).	■ "Deployment options" ■ Appendix A, "Planning forms"
☐	Plan RLC port assignments.	"Connection Information—16 ports" or "Connection Information—32 ports", depending on your RLC.
2. PBX configuration		
☐	Configure the PBX to recognize each RLC as an XDLC.	documentation for your PBX.
☐	Verify that the PBX recognizes each RLC as an XDLC.	

RLC Installation Checklist

Page 3 of 6

Check	Task	For details, refer to
☐	If you want to use the PSTN to route calls, ensure that ISDN BRI or PRI trunks are installed and configured on the PBX for voice and data.	configuration on your PBX.
☐	Ensure that there is sufficient capacity on the trunks for the extra traffic involved in remote service operations.	configuration on your PBX and the <i>Remote Office Network Engineering Guidelines</i> (NTP 555-8421-103). You can obtain this document online at the following address: www.nortelnetworks.com
☐	Configure a voice port (or data port for MCA) on the PBX for each remote user. (These ports are associated with Remote ports on the RLC.)	documentation for your PBX.
☐	Configure a data port (or voice port for 911x modem) on the PBX for each remote unit connection. (These ports are associated with Network ports on the RLC.)	
3. Hardware and software installation		
☐	Install DSP application modules on the RLC, if required.	"Installing DSP application modules".
☐	Install and cable each RLC.	■ "To install a RLC" ■ "To cable a RLC"

RLC Installation Checklist

Page 4 of 6

Check	Task	For details, refer to
☐	Install the software from the product CD-ROM or download the software from the Nortel Networks web site.	"Installing the software".
4. RLC configuration		
☐	Configure the IP address, subnet mask, and default gateway on the RLC.	"Using the Configuration Wizard to perform initial configuration".
☐	If you want to use the PBX's administration terminal to administer the RLC, configure the IP address and subnet mask of the RLC's ELAN port.	"IP Configuration".
☐	Configure the following items, as required, to create the communication paths between the RLC and the remote unit: ■ IP network: remote unit's IP address ■ PSTN: remote unit's telephone number ■ security level and, if required, security identifier	■ "Using the Configuration Wizard to perform initial configuration" ■ "To configure remote connection settings"
☐	Configure a Remote port on the RLC for each user. Note: The process of creating the PSTN communication path with the Configuration Wizard creates a Network port for each remote unit.	Chapter 6, "Configuring the Reach Line Card".

RLC Installation Checklist

Page 5 of 6

Check	Task	For details, refer to
☐	Configure an Online/Offline Schedule for each remote unit, if required.	“Configuring an online/offline table”. Note: A blank online/offline schedule can be found in the Online/Offline Table section of Configuration Manger.
5. Remote unit configuration		
☐	Ensure that the remote unit is configured with the information it needs to establish connections with the RLC.	the <i>Installation and Administration Guide</i> for the remote unit.
☐	Ensure that a station is configured for each remote user.	the <i>Remote Office 9150 Installation and Administration Guide</i> (NTP 555-8421-215), or the <i>Remote Office 911x Series Installation and Administration Guide</i> (NTP 555-8421-220), depending on remote site equipment.
6. Network configuration		
☐	Configure network devices ■ so that voice traffic is not constrained or congested ■ to maximize network efficiency for Voice over IP service	■ your data network administrator ■ the <i>Remote Office Network Engineering Guidelines</i> (NTP 555-8421-103) You can obtain this document online at the following address: www.nortelnetworks.com

RLC Installation Checklist

Page 6 of 6

Check	Task	For details, refer to
☐ ☐	Ensure that voice calls can be sent or received over the following: ■ IP network ■ PSTN	■ your data network administrator ■ your telecom network administrator
☐ ☐	Ensure that processing of voice and data traffic over the IP network performs as expected. Adjust QoS transition settings, if required.	■ your data network administrator ■ your telecom network administrator ■ the <i>Remote Office Network Engineering Guidelines</i> (NTP 555-8421-103) You can obtain this document online at the following address: www.nortelnetworks.com
7. Testing		
☐	PING the RLC to ensure that it is recognized as a device on the network.	"Testing the connections".
☐	Ensure that calls can be made and received on each RLC port.	"Testing the connections".
8. Administration		
☐	Plan for administration training and technical support.	■ Chapter 7, "Administration" ■ Chapter 8, "Troubleshooting"

Note: The RLC and Configuration Manager software are Year 2000 compliant.

System resources management

The RLC offers the following methods to manage system resources:

- QoS Transitioning Technology
- Host connection management
 - Configurable trunk connection accessibility (permanent or on-demand)
 - Call timers for managing of on-demand trunks
- Online/offline scheduling
- Configurable security

QoS Transitioning Technology

Traffic congestion often results in poor voice quality or lost connections on IP networks. For a description of the RLC's QoS Transitioning Technology, refer to "Adjustable quality of service using QoS Transitioning Technology" on page 15.

For detailed information on configuring QoS Transitioning Technology thresholds, refer to "Configuring Quality of Service" on page 182.

Host connection management

Manage connections to the host PBX in the following three ways:

- Configure an Online/Offline table for the remote site to determine when it can and cannot place or receive calls through the host PBX.
- Define a trunk connection as permanent or on-demand so that it is one of the following:
 - Always connected (permanent)
 - Connected when bandwidth required (on-demand)
- Define minimum call duration and idle timers to address call-establishment and PSTN charges, if the trunk connection is defined as on-demand.

Call-on-demand

The RLC supports full call-on-demand (COD) capability. In COD mode, the RLC does not establish a connection to the remote site until the remote unit places a call to a host DN. For further information on the RLC's COD functionality, see "Call on-demand" on page 20.

Online/offline schedule

You can configure an online/offline schedule on the RLC to control when remote sites can place and receive calls through the host PBX.

Note: Online/offline schedules configured for Remote Office 9150 units affect all users connected to that unit.

Configure offline entries for the following situations:

- to restrict remote users from placing or receiving calls at certain times, such as during evenings and weekends
- to eliminate unwanted telephone access charges by preventing remote sites from staying online permanently

When the RLC processes an offline entry, it instructs the remote site to go offline for a certain number of hours and minutes. That number is the difference between the offline entry being processed and the next online entry.

For example, suppose you configure an offline entry for 6:00 p.m. and the next online entry for 9:00 a.m. the next day. When the RLC processes the 6:00 p.m. entry, it instructs the remote site to go offline for 15 hours.

When going offline, the system activates a timer at the remote site. When the timer expires (in the example above, at 9:00 a.m.), the remote site initiates a "going online" request to the host PBX. If the RLC successfully receives the request, the remote site and its telephones go online.

Changing the online/offline mode

You can put the remote site into online or offline mode at any time. Simply dial one of two special prefix (SPRE) codes at any remote site telephone set. Configure the online SPRE and offline SPRE codes through Configuration Manager. These codes must not conflict with the dialing plans used at the host PBX. See “9150 System Configuration” in the *Remote Office 9150 Installation and Administration Guide* (NTP 555-8421-215), for information on configuring SPRE codes.

Configurable security

Security settings apply to the RLC on a remote unit basis. Enter this information through Configuration Manager. Refer to “Remote Connection Configuration” on page 171.

The RLC offers three levels of security. For a detailed description of the RLC’s variable the security levels, refer to “Multiple security levels” on page 17.

Data network security

The RLC does not provide for data network security. To provide security on the data network, implement security on the data network devices.

System security

Two layers of security protect the RLC and its remote sites:

- **Local password**
You must enter the local password when starting Configuration Manager software. If the person attempting to use Configuration Manager does not have the password, the Remote Office system blocks that person from accessing any Remote Office nodes.
- **Node password**
Users must enter the node password before Configuration Manager displays the configuration of the logged-on node and allows modification of that configuration.

ATTENTION!

Nortel Networks recommends that users retain the factory-set password until the system is up and running smoothly.

Lost or forgotten passwords

If you lose or forget your RLC or Configuration Manager password, contact your Nortel Networks supplier for assistance.

Network considerations

When you implement an RLC-based remote service system, consider the ways that the new equipment effects your current telecommunications and data networks.

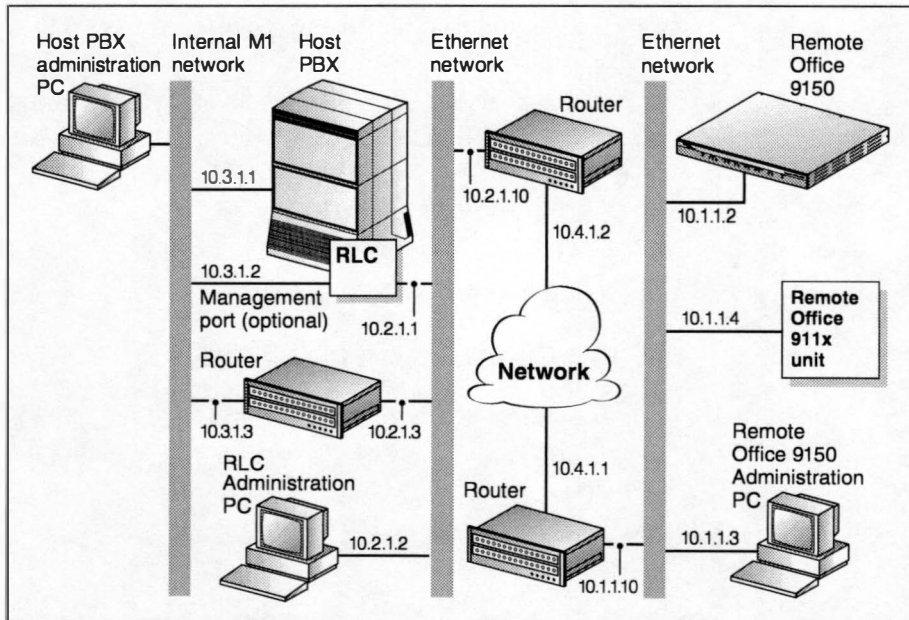
IP addressing and routing

To place and receive calls over the IP network, the RLC must have:

- A physical connection to the IP network
- A unique IP address and subnet mask

Network diagram

The following diagram shows the RLC's position in an IP network.



G029

Quality of service

The routers used on your IP network must handle voice traffic while introducing little or no congestion and few delays into the network. Network congestion or excessive delay adversely effects voice quality.

Trunks and dialing plans

To obtain an outside line on the local PSTN, users dial local trunk-access SPRE codes. The SPRE codes configured for remote sites must not conflict with the dialing plans used by the host PBX. Conflicts result in end-users not being able to place outgoing calls through the local PSTN.

Call blocking

The voice processing capacity of a remote system depends on the number of DSP application and trunk interface modules installed at the host and remote sites. Voice processing capacity defines the number of calls that can be active simultaneously and the amount of bandwidth the site can access.

Reducing call blocking in PSTN mode

Remote Office 9150 units use ISDN BRI trunks in PSTN mode. To reduce call blocking in the PSTN mode at the host location, you must increase the number of trunks available to the RLC.

Reducing call blocking in Voice over IP mode

One DSP application module provides the ability to support eight simultaneous Remote Office calls. To reduce call blocking for Voice over Internet Protocol (VoIP) calls, increase the number of DSP resources in your system. Do this at the host (RLC) site and, if the remote unit is a Remote Office 9150 unit, at the remote site. You can install up to four DSP application modules on a Remote Office 9150 unit and up to four DSP application modules on an RLC.

Calculating system requirements

For help in determining how many DSP application modules you need to install to reduce or eliminate call blocking, refer to “DSP requirements” on page 45 and the RLC System expansion worksheet on page 293.

Administration PC

Install the Windows-based RLC administration software on a PC in the Remote Office network. This section describes options for connecting an administration PC to the RLC. It also describes the hardware and software requirements of the administration software.

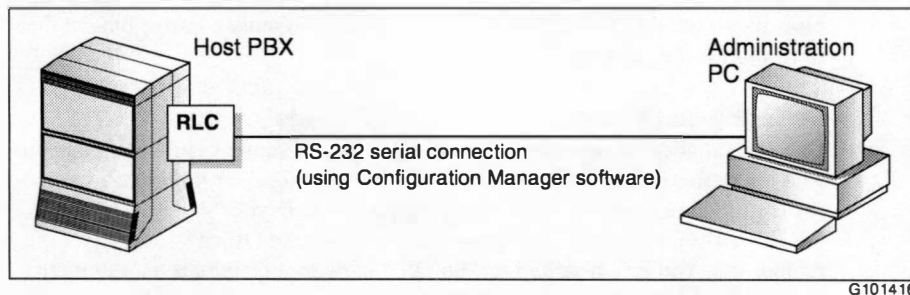
Connection options

The RLC product includes the Configuration Manager software that enables you to configure, administer, and upgrade the RLC. Perform these tasks over one of the following connections:

- RS-232 serial connection
- 10BaseT Ethernet connection

Serial connection

Use the serial connection when you first install and configure the RLC. You must establish a serial connection to the RLC, as shown in the illustration below, to enter the IP interface information.

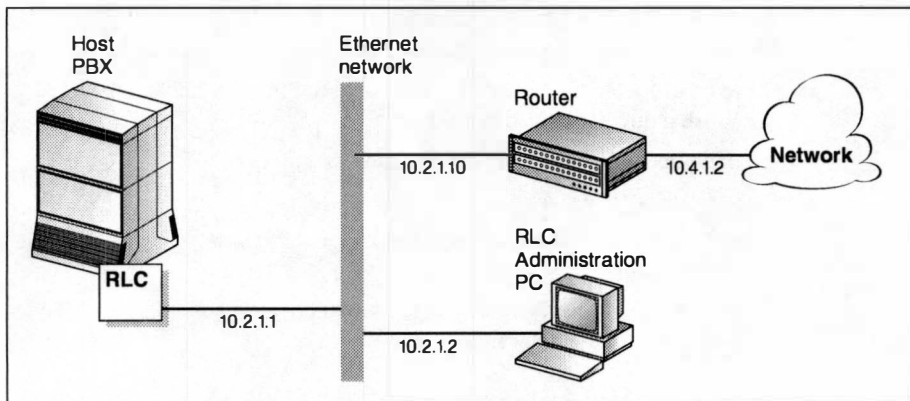


You can continue using the serial connection for ongoing administration of the RLC if you prefer.

Ethernet connection

Configure the RLC's IP interface information to allow calls to be routed between the RLC and remote units. This also allows RLC administration to take place over the IP network from a remote location.

Remote administration of the RLC means you can install the administration PC in a location different from that of the RLC.



G031

Administering multiple nodes

If you are responsible for administering the RLC on the host PBX and one or more remote units, you can access the RLC and the remote unit from anywhere on the network.

Windows PC requirements

To use Configuration Manager, the administration PC must:

- be an IBM-compatible PC
- use a Windows 95, 98, or NT operating system with the Microsoft TCP/IP networking component installed
- be equipped with a CD-ROM drive
- be equipped with a 10BaseT Ethernet interface card
- have an available COM port if you wish to use the RS-232 serial port to establish a direct serial connection
- be equipped with a pointing device, such as a mouse
- use Microsoft's IP stack
- have 32 MBytes of RAM for Windows 95 and 98, or 64 MBytes of RAM for Windows NT
- have 48 MBytes of available storage for Windows 95 and 98, or 64 MBytes of available storage for Windows NT

Trivial File Transfer Protocol server

Firmware upgrades and configuration uploads require that the administration PC have a TFTP server application installed. The administrator must know the TFTP server's IP address in the network. In other words, the IP address of the administration PC.

You can use any TFTP server application. These applications are available free of charge on the Internet.

Year 2000 compliance

The RLC and Configuration Manager software are Year 2000 compliant. However, ensure the administration PC is Year 2000 compliant by verifying that the Windows operating system meets the compliance requirement listed in the following table:

Operating system	Year 2000 compliance requirement
Windows 95	Version 95b
Windows 98	OK as is
Windows NT Workstation	Service Pack 5

Meridian Administration Tools and Configuration Manager

Nortel Networks does not guarantee that Meridian Administration Tools (MAT) and the Remote Office Configuration Manager can operate simultaneously on the same administration PC. Simultaneous running of these two applications has not been tested and is, therefore, not supported.

Planning for future growth

The RLC can change as your telecommunication needs change or grow. When determining remote port needs for your network, it is important to consider the number of users and estimated growth at each site in the network.

Adding DSP modules

The RLC ships with enough built-in DSP resources to support up to eight simultaneous telephone calls without the addition of any DSP application modules. For information on increasing the voice processing capability of the RLC, see “DSP requirements” on page 45.

For help determining how many DSP application modules you need to meet your call-processing expectations, see the “System expansion worksheet” on page 293. For instructions on installing additional DSP modules, see “Installing DSP application modules” on page 72.

Deployment options

You can install and configure the RLC on the host PBX and remote units at remote sites with the following network capabilities:

- only the IP network (Voice over IP)
- only the PSTN (for example, ISDN BRI trunks)
- both networks (required for QoS Transitioning Technology functionality)

If you choose not to use both networks initially, this section suggests how you can gradually phase-in Voice over IP and QoS Transitioning Technology functionality.

ATTENTION!

Even if you plan to route calls over the PSTN only, you must assign an IP address and IP gateway to the RLC and remote units to allow remote administration.

Port and station assignment

Regardless of which network you use initially to route calls, you must plan RLC port and remote site user station assignments. Assign a single user to each RLC port, unless you are using the RLC's port sharing functionality (refer to "Port sharing options" on page 16). Use the following forms to plan port and station assignment:

- "Reach Line Card Connection Information—16 ports" on page 278
- "Reach Line Card Connection Information—32 ports" on page 283

Implementing PSTN mode

In a scenario involving the PSTN mode only, the PSTN processes all incoming and outgoing calls as follows:

IF the call is to or from the	THEN the call is in
host PBX,	host-controlled mode.
other PSTN customers,	local-controlled mode.

To implement PSTN mode, you must complete the following steps:

- 1 Determine how many simultaneous calls you want to process over the PSTN.

Note: Include all single-user Remote Office 911x series and Meridian Digital Telephone IP Adapter sites along with all multi-user Remote Office 9150 sites that use the same RLC in this calculation.

If the remote unit is a Remote Office 911x series unit, configure the appropriate number of DSP resources on the RLC for 911x use. For the necessary procedure, refer to Chapter 6.

- 2 Arrange for PSTN lines to each remote site if these lines are not already present.
- 3 Install up to four DSP application modules on the RLC to increase voice processing capability if needed.

Note: RLCs do not ship with DSP application modules installed.

- 4 Install ISDN BRI trunk interface and DSP application modules on each Remote Office 9150 unit if needed. Install up to four ISDN BRI modules and up to three DSP application modules.

Note: Remote Office 9150 units do not ship with trunk interface modules or DSP application modules installed.

- 5 Obtain the telephone number of the RLC port that the remote unit is assigned to. Configure this telephone number on the remote unit—the remote unit uses it to establish connections with the RLC.

- 6 For each remote unit, obtain the information for each PSTN line from the remote unit's telephone service provider. Configure this information on the remote unit to establish the trunk interface with the PSTN.

Note: For Remote Office 9150 units, remember to get this information for each ISDN BRI line.

- 7 Identify the telephone number assigned to the remote unit. Configure this telephone number on the RLC—the RLC uses it to establish connections with the remote site.

Implementing Voice over IP mode

In Voice over IP (VoIP) mode, the system processes all incoming and outgoing calls across the IP network through the host PBX. The system routes calls made to external parties to the PSTN using host PBX trunks. Calls processed through the host PBX are referred to as *host-controlled calls*.

Note: Local PSTN calls at Remote Office 9150 sites require access to ISDN BRI lines and the installation of ISDN BRI application modules in the Remote Office 9150 unit. Local PSTN calls made at Remote Office 9110 and Remote Office 9115 sites use analog, POTS lines. All calls not routed through the host PBX, whether ISDN or POTS, are referred to as *locally controlled calls*.

To implement VoIP mode for host-controlled calls:

- 1 Determine how many simultaneous calls you want to process. This helps you to determine how many DSP application modules to install on the RLC. To do this, complete the RLC System expansion worksheet on page 293.
- 2 Install DSP application modules on the RLC, if needed.
- 3 Obtain the IP address assigned to the remote unit. Configure this IP address on the RLC—the RLC uses it to establish connections with the remote unit.
- 4 Obtain the IP address assigned to the RLC. Configure this IP address on the remote unit—the remote unit uses it to establish connections with the RLC.

- 5 Run this stage with a small number of users at first. Before applying VoIP mode to your entire remote network, you must ensure that one of the following is true:
- Your IP network can handle the addition of remote network traffic.
 - You can identify the kinds of configuration adjustments you need to make to the IP network so that it can handle the additional traffic.

When you are satisfied with the IP network performance, continue with QoS Transitioning Technology implementation.

Implementing Quality of Service Transitioning Technology

To implement the QoS Transitioning Technology, you must understand characteristics of your IP network, such as:

- when the network experiences busy times
- how much traffic the network processes (during normal and busy traffic periods)
- how to evaluate and adjust your network's QoS

Consult with your data network administrator. Refer also to the *Remote Office Network Engineering Guidelines* (NTP 555-8421-103). Refer to "Related information products" on page xxii for information on obtaining this document.

Once you understand this information, determine the QoS settings that you want, then configure them on each RLC port. For instructions, refer to "Configuring Quality of Service" on page 182.

If IP mode is not the first stage in your network implementation, run this stage with a minimal number of users until you are sure that QoS on your IP network is acceptable. When you are satisfied with QoS transitioning performance, deploy the capability to the entire network.

If you are configuring QoS Transitioning Technology for Remote Office 911x series units, on the RLC you must configure at least one DSP device with the DSP load "911X". Each DSP device configured with the DSP load "911X" supports four modem channels.

Chapter 3

Installing the RLC

In this chapter

General safety	70
Installing DSP application modules	72
Identifying the cables	74
Installing the Reach Line Card	78
Verifying the installation	81
Configuration Manager software installation	82
Using the Configuration Wizard to perform initial configuration	83
Testing the connections	96

General safety

This section describes general safety guidelines recommended by Nortel Networks, and tools needed for installation. Follow the safety guidelines and recommendations in this chapter whenever you perform installation or maintenance tasks on the RLC.



CAUTION

Risk of data loss or equipment damage

Electrostatic discharge (ESD) effects the performance and decreases the useful life of system components. It can seriously damage component parts, such as RLCs and DSP application modules.

Precautionary messages

This guide provides warnings related to hardware installation and handling, such as the preceding caution. For a description of these warnings, refer to “Conventions used in this guide” on page xx.

Required tools for hardware installation

Items needed for hardware installation include the following:

- antistatic ESD wrist strap (recommended)
- phillips-head screwdriver
- slot-head screwdriver
- pen or pencil for
 - noting cable lengths
 - labeling cables
- cable-tie wraps
- cable identification labels
- tape measure

Required tools for software installation or upgrade

Items needed for software installation or upgrade include the following:

- *Remote Office Product CD-ROM*
- network connection to the Nortel Networks website for obtaining upgrade files

Installing DSP application modules

Install DSP application modules (NTDR73xx) in the expansion slots on your RLC. This increases the number of simultaneous ports, and telephone lines, that you can use at remote sites. To add DSP application modules to your RLC, follow these procedures:

- 1 Determine the number of DSP application modules that meets your needs using the System expansion worksheet on page 293.
- 2 Install DSP application modules using the procedure on page 73.

Determining how many DSP application modules to add

To determine the number of DSP application modules your RLC needs, refer to the System expansion worksheet on page 293. For more information on how DSP application modules fit into your Remote Office system, refer to “DSP requirements” on page 45.

After receiving the DSP application modules from Nortel Networks, install them according to the procedure found under “Installing DSP application modules” on page 73.

Handling DSP application modules

Before beginning the installation and configuration process, review “General safety” on page 70. Follow the safety precautions and warnings found there to protect your investment in your telecommunications network.



CAUTION

Risk of data loss or equipment damage

Be certain you are properly grounded before handling DSP application modules or the RLC.

Installing DSP application modules

To install DSP application modules:

- 1 Clear a flat, static-free work area with sufficient space to hold your RLC and DSP application modules.
- 2 Place the DSP application modules in the work area.
Note: Keep the DSP application modules in their antistatic bags.
- 3 Move the RLC from the host PBX to the work area.
- 4 Remove a DSP application module from its antistatic bag, holding it by its edges, with the insertion tabs facing down.
- 5 Insert the tabs into a pair of expansion slots on the RLC. (Refer to the illustration on page 5 for location of expansion slots.) The tabs snap into place when fully inserted. Visually inspect each tab to make sure that there is no gap and that the tab is fully inserted.

Identifying the cables

Cable your RLC according to the needs of your system. The following table identifies the cables available from Nortel Networks according to the connectivity provided by each.

IF you use the	THEN you can connect to
RLC Multi-I/O cable–Basic (NTDR79xx),	■ the PSTN. ■ the Voice over Internet Protocol (VoIP) network.
RLC Multi-I/O cable–Enhanced (NTDR80xx),	■ the PSTN. ■ the Voice over Internet Protocol (VoIP) network. ■ locally connected telephones.

Pin-out tables for these cables are located in Appendix C, “Pin-out tables for RLC Multi-I/O cables”.

RLC Multi-I/O cable–Basic (NTDR79xx)

The RLC Multi-I/O cable–Basic provides three connections. Any number of RLCs in any card slot can use the Basic cable.

The following table outlines the connections provided by the RLC Multi-I/O cable–Basic.

The connector labeled	is a	that transmits	and connects to the
P1	25-pair connector (female)	all signals	I/O panel.
Note: For a 32-port RLC, insert P1 into the socket for the first card slot occupied by the RLC.			
P2	DB-15 connector (male)	10BaseT signaling	CLAN Ethernet (customer LAN on the network).
Note: P2 requires a DB-15 to RJ-45 converter (shipped with the cable).			
P3	DB-9 connector (female)	RS-232 signaling	serial port to admin PC for administration and maintenance.

Refer to page 9 for an illustration of the RLC Multi-I/O cable–Basic.

RLC Multi-I/O cable–Enhanced (NTDR80xx)

The RLC Multi-I/O cable–Enhanced provides six connections. You can purchase the RLC Multi-I/O cable–Enhanced separately from Nortel Networks.

Note: Special rules apply if using more than one RLC Multi-I/O cable–Enhanced in one Option 11 cabinet. For further details, contact your Nortel Network distributor.

The following table describes the connectors of the RLC Multi-I/O cable–Enhanced:

The connector labeled	is a	that transmits	and connects to the
P1	female 25-pair connector	all signals	I/O panel.
Note: If you are using a 32-port RLC, insert P1 into the socket for the first of the two card slots occupied by the RLC.			
P2	male DB-15 connector	10BaseT signaling	CLAN Ethernet (customer LAN on the network).
Note: In North America, P2 requires a DB-15 to RJ-45 converter (shipped with the cable). Outside North America this plug is a female RJ-45 connector.			
P3	female DB-9 connector	RS-232 signaling	serial port to admin PC for administration and maintenance.
P4	male DB-15 connector	10BaseT signaling	ELAN Ethernet (host PBX's embedded LAN).
Note: In North America, P4 requires a DB-15 to RJ-45 converter (shipped with the cable). Outside North America this plug is a female RJ-45 connector.			
P5	male 25-pair connector	TCM signaling	cross-connect to local telephones.
P6	male DB-25	(For future use.)	

Notes:

- Refer to page 11 for an illustration of the RLC Multi-I/O cable–Enhanced.
- The illustration on page 13 shows the RLC Multi-I/O cable–Enhanced used in installations outside North America.

Installing the Reach Line Card

The process of installing the Reach Line Card (RLC) involves:

- preparing the switch
- placing the RLC into its slot
- connecting the cables to the RLC

In systems with multiple RLCs, the process is the same for each one.

Preparing for installation

Configure the RLC's slot as if it were to hold an Extended Digital Line Card (XDLC). Refer to the documentation specific to your PBX for the exact procedures.

Split-slot wiring

If you use a NT8D37AA IPE cabinet, refer to the important note concerning the wiring of these cabinets on page 3.

Installing an RLC

To install an RLC:

- 1 Insert the RLC into its card slot.
Ensure that the tips of the ejector tabs are inside the front edges of the shelf when the card is fully inserted.
- 2 Lock the RLC into position by pushing the handles toward one another until they touch the faceplate.
If you meet with inappropriate resistance, stop and reposition the card.
Refer to "LED indicators" on page 7 for the sequence of events that signify a successful RLC installation.
- 3 Verify that the host PBX recognizes the presence of the RLC. (Refer to the documentation specific to your PBX for exact procedures.)

Connecting the cables to an RLC

To connect the cables for an RLC:

- 1 Plug **P1** of the RLC Multi-I/O cable (Basic or Enhanced), the female 25-pair connector, into the 25-pair shelf connector associated with the slot occupied by the RLC.

Note: If you are connecting the cables to a 32-channel RLC, use the shelf connector associated with the first of the two slots occupied by the RLC.

IF installing the**THEN proceed to**

RLC Multi-I/O cable—Basic, step 2.

RLC Multi-I/O cable—Enhanced in step 2.
North America,

RLC Multi-I/O cable—Enhanced in step 3.
a location other than North
America,

- 2 Plug **P2**, the male DB-15 connector (if using the Enhanced cable, this is the first male DB-15 connector), into a DB-15 to RJ-45 adapter (NT7R93CA).

Note: The RLC Multi-I/O cable—Enhanced ships with this adapter. This adapter is not an active transceiver.

- a. Plug one end of a *shielded* (to meet CISPR B requirements) CAT 5 data cable of sufficient length to reach your Ethernet hub into the other side of the DB15 to RJ45 adapter connected to P2.
- b. Plug the other end of the CAT5 data cable into your Ethernet hub.
- c. Proceed to step 4.

- 3 Plug **P2**, the male DB-45 connector into a female RJ-45 connector at one end of a *shielded* (to meet CISPR B requirements) CAT 5 data cable of sufficient length to reach your Ethernet hub.

- a. Plug the other end of the CAT5 data cable into your Ethernet hub.

- 4 Plug **P3**, the female DB-9 connector of the RLC Multi-I/O cable (Basic or Enhanced), into the Remote Office administration PC.

IF installing the**THEN proceed to**

RLC Multi-I/O cable–Basic,

“Verifying the installation” on page 81.

RLC Multi-I/O cable–Enhanced in step 5.
North America,RLC Multi-I/O cable–Enhanced in step 6.
a location other than North
America,

-
- 5 Plug **P4**, the second male DB-15 connector of the RLC Multi-I/O cable–Enhanced, into a DB15 to RJ45 adapter (NT7R93CA).

Note: The RLC Multi-I/O cable–Enhanced ships with this adapter. This adapter is not an active transceiver.

- a. Plug one end of a *shielded* (to meet CISPR B requirements) CAT 5 data cable of sufficient length to reach your Ethernet hub into the other side of the DB15 to RJ45 adapter connected to P2.
 - b. Plug the other end of the CAT5 data cable into your Ethernet hub.
 - c. Proceed to “Verifying the installation” on page 81.
- 6 Plug **P5**, the second 25-pair connector, into the cross-connect device serving the local telephones that you want to attach to RLC ports not needed for remote service purposes.
- 7 P6 is reserved for future use.

Verifying the installation

Once you have finished installing your RLC and connecting the cables, verify that you have completed these procedures properly according to the indications discussed below.

Indications of proper installation

An RLC automatically performs a self-test when inserted into its card slot. A successful self-test indicates proper installation. The Maintenance LED confirms a successful self-test by:

- blinking three times
- turning off (when enabled by the switch)
- remaining off (if enabled by the switch)

Note: Refer to “LED indicators” on page 7 for a further explanation of LED behavior at startup.

Indications of proper cable connections

The ability to successfully log on to the RLC using Configuration Manager software indicates proper cable connections at the RLC. To perform this task, install the software first (refer to page 82). Once this task is completed, continue with “Starting Configuration Manager” on page 84.

Confirm the cable connections before attempting the troubleshooting procedures.

Note: If the RLC cables are properly connected and you still cannot log on, refer to Chapter 8, “Troubleshooting”.

Configuration Manager software installation

Use Configuration Manager software to configure and administer the RLC. This software arrives on the CD provided in the package. You must install this software on the administration PC to configure and administer the RLC and the Remote Office system.

What's next?

After you install the software on the administration PC, start Configuration Manager and run the Configuration Wizard. The Configuration Wizard allows you to perform initial configuration quickly and easily.

For instructions, refer to “Using the Configuration Wizard to perform initial configuration” on page 83.

Note: Leave DLL files installed by the Configuration Manager InstallShield in the Windows system directory. Do not move these files to any other directory.

Using the Configuration Wizard to perform initial configuration

The Configuration Wizard option in Configuration Manager allows you to configure the minimum information needed for establishing communications between the RLC at the host site and the following remote-site products:

- Remote Office 9110
- Remote Office 9115
- Remote Office 9150
- Meridian Digital Telephone Internal IP Adapter
- Meridian Digital Telephone External IP Adapter

The Configuration Wizard provides only a subset of the full configuration settings available in Configuration Manager. However, by using the Configuration Wizard, the RLC can be up and running within 10 minutes.

You can use the Configuration Wizard in offline mode or while connected and logged on to the RLC (online mode).

What you can configure with the Configuration Wizard

The Configuration Wizard allows you to configure the following elements:

- the RLC's IP address, subnet mask, and default gateway

This information must be valid for your IP network.

Note: If you do not plan to use the IP network to route calls, you must still enter this information for administration purposes. If you do not have an IP network in place, the procedure on page 89 provides sample information.

- for voice over IP capability:
 - the IP addresses for each remote unit connected to the RLC
- for PSTN capability:
 - the RLC port used for connection to the remote unit
 - the telephone number of the remote unit

Ensure that you have this information ready before you begin.

ATTENTION

If, after completing configuration with the Configuration Wizard, you want to modify any settings, you must use Configuration Manager.

Starting Configuration Manager

To start Configuration Manager:

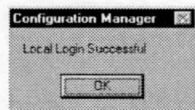
- 1 Click on Start → Programs → Remote Office → Configuration Manager.

Result: Configuration Manager opens and displays the Local User Authentication dialog box, similar to the following, prompting you for the login name and password:



- 2 Enter **admin** in the Login Name field.
- 3 Enter **root** in the Password field.
- 4 Click on the **OK** button.

Result: The Configuration Manager dialog box displays informing you of a successful log on.



- 5 Click on the **OK** button.

Result: The Configuration Manager dialog box disappears.

- 6 Do one of the following:

**IF you want
to perform an**

THEN

offline configuration,

- Choose View › Device Type › RLC.
- Continue with “Performing configuration with the Configuration Wizard” on page 88.

online configuration,

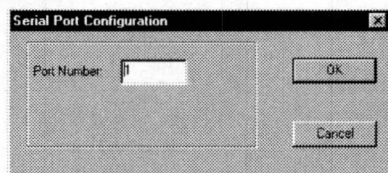
continue with “Establishing a serial connection”, below.

Establishing a serial connection

To establish a serial connection:

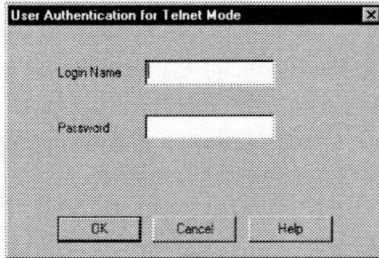
- 1 From the Menu Bar, choose Connect → Logon Unit → Serial.

Result: The Serial Port Configuration dialog box displays, similar to the following:



- 2 Enter the COM port number the unit is connected to in the Port Number field, and then click on the **OK** button.

Result: The User Authentication for Telnet Mode dialog box displays, similar to the following:



- 3 Enter **guest** in the Login Name field.
- 4 Enter the default password, **guest123**, in the Password field.

Note: Nortel Networks recommends that you do not change the password until your system is up and running.

Result: Configuration Manager initiates a connection attempt and displays the following message:

Trying Connection

IF the logon attempt THEN

failed, the following message displays:

10060 SERIAL CONNECTION FAILED

Go back to step 1.

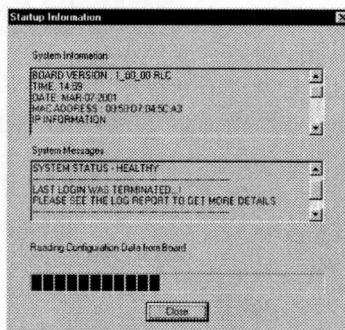
IF the logon attempt THEN

is successful,

the User Logged In dialog box displays.

Click on the **OK** button.

Result: The Startup Information dialog box displays, similar to following:



Messages similar to the following appear above the progress bar at the bottom of the dialog box:

- Reading Hardware Information
- Reading DSP Load Data
- Reading Configuration Data

These messages indicate that Configuration Manager is obtaining the unit's configuration information from Flash memory.

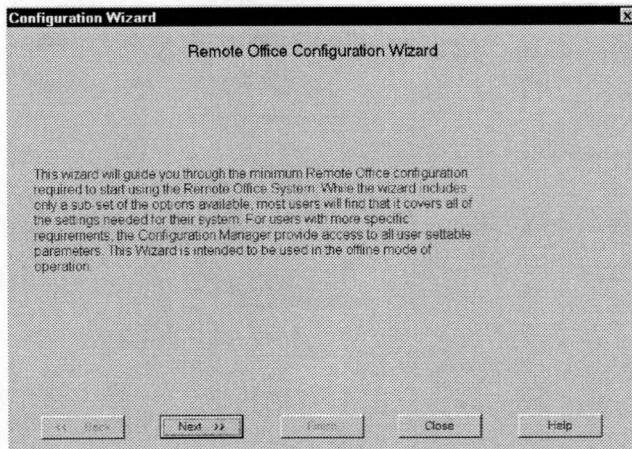
Click on the **Close** button.

Performing configuration with the Configuration Wizard

To perform configuration with the Configuration Wizard:

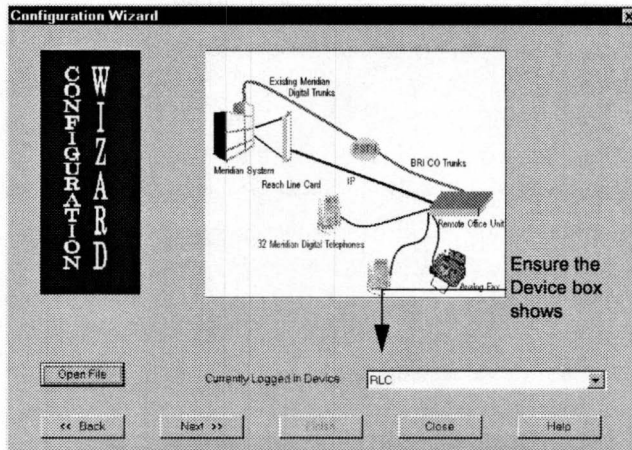
- 1 From the Menu Bar, choose Configuration Wizard.

Result: The Configuration Wizard screen displays, similar to the following:



- 2 After reviewing the message, click on the **Next** button.

Result: The Configuration Wizard screen displays, similar to the following:



- 3 Verify that the Currently Logged in Device drop down box shows RLC. If it does not show RLC, select RLC from the drop down list.
- 4 Click on the **Next** button.

Result: The Local Unit Configuration dialog box displays. A completed example is shown on page 90.

- 5 Complete the fields in this dialog box as described in the following table:

Field	Description
Enter a node name that identifies the unit	Enter a name to describe the RLC you are configuring.
Enter the local IP Address of the unit	Enter the IP address assigned to the RLC. Note: The system requires that you enter an IP address. If you are using PSTN only, enter the following: 1.2.3.4.

Field	Description
Enter the Local IP Mask of the unit	Enter the subnet mask. Note: The system requires that you enter an IP address. If you are using PSTN only, enter the following: 255.255.0.0 .
Enter the Local IP Gateway of the unit	Enter the IP address of the gateway between the RLC and the network. Note: The system requires that you enter an IP address. If you are using the PSTN only, enter 1.2.3.5 , as both the IP address on the administration PC and gateway on the RLC.

The following is a completed example:

The IP information allows you to administer the RLC from any location on the

- 6 Click on the **Next** button.

Result: The Set the Remote Unit information dialog box displays. A completed example is shown on page 93.

- 7 Complete the fields on this screen as described in the following table:

Field	Description
Set the Number of Remote Units	Enter the number of remote units you plan to connect to this RLC.
Set the Unit Number of the Remote unit	Enter the number that uniquely identifies the remote unit record you are configuring. Note: You must give each unit that is connected to the same RLC a unique unit record number. Do not confuse this number with the unit ID (described below).
Wish to Enable IP Voice Connection to Remote	■ Click on the Yes option button if using the IP network to route calls. Then, enter the remote unit's IP address. ■ Click on the No option button if not using the IP network. Configuration Manager dims the IP Address boxes.

Field	Description
Wish to Enable PSTN Voice Connection to Remote	■ Click on the Yes option button if using the PSTN to route calls. Then complete the following steps: - a Enter the number of the RLC port that you want to dedicate for connections to this remote unit. Note: The port must be a PBX data port. - b Enter the telephone number that you must dial to connect to the remote unit. The telephone number can include the following digits or characters: 0 through 9, #, *, comma (,), period (.), and dash (-). ■ Trunk access digit delimiter: “#” (pound/number sign) ■ Caller ID separator and 1/2 second delay: “,” (comma) ■ Caller ID separator: “.” (period) ■ null separator: “-” (dash) Refer to “Configuring 10-digit ISDN numbers” on page 175 for more information. ■ Click on the No option button if not using the PSTN. The PSTN Voice Connection boxes are dimmed.
8	Click on the Press to update the remote unit list button. Result: The information entered for this remote unit appears in the list of configured remote units in the lower half of the Set the Remote Unit information dialog box.

The following is a completed example:

Click on the **Yes** option button to allow voice calls over IP, then enter the remote unit's IP address.

Set the Remote Unit information

Set the Number of Remote Units: 1 Set the Unit Number of the Remote unit: 1

Wish to Enable IP Voice Connection to Remote: ☒ Yes If Yes, Enter the IP Address of the Remote Unit: 192 168 142 201

Wish to Enable PSTN Voice Connection to Remote: ☒ Yes Enter the first data port to dial to the 9150: 16 Enter the PSTN Number of the 9150: 4542

This displays the list of Remote Units that have been configured. Right click on the list to remove any Remote Units configured. Press to update the remote unit list

Unit ID	IP Status	IP Address	PSTN Status	Remote PSTN Number	Local Trunk Port
1	Y	192.168.142.201	E	4542	16

<< Back Next >> Finish Close Help

Click on the **Yes** option button to allow voice calls over the PSTN, then enter the remote unit's phone

This table allows you to configure connections for more than one remote unit.

- 9 Repeat steps 7 and 8 for each remote unit you need to configure.
- 10 Click on the **Next** button.

Result: The following screen displays:

Configuration Wizard

You have successfully configured the board. You have two options to choose from.
 You could use the Save to Flash option which will write the configured information onto the flash.
 You could also save the configuration onto a file which you could reload later onto the Configuration Manager.

<< Back Next >> Save to Flash Save to File Close Help

- 11 Do one of the following:

IF you are performing an THEN

offline configuration,

- 1 Click on the **Save to File** button.

Result: Configuration Manager prompts you to specify the directory path and file name for the configuration file.

- 2 Specify the directory path and file name for this configuration.

Note: The file name automatically defaults to the name you entered as the node name.

- 3 Ensure the Files of type box shows Text File (*.TXT).

- 4 Click on the **Save** button to complete the Save to File.

Result: The file is saved, then you are asked if you want to configure another board. If you do, click on the **Yes** button and continue with step 3 on page 89.

- 5 You can open the information in this file in Configuration Manager, then send and save the file in the RLC's flash memory at another time. For instructions, refer to "Working with configuration files" on page 132.

IF you are performing an THEN

online configuration,

- 1 Choose Upload/Download → Save to Flash from the Menu Bar.

Result: Configuration Manager writes the information entered to the flash memory of the RLC you are configuring.

If successful, Configuration Manager displays the following message:

Data Sent Successfully

Note: Nortel Networks recommends that you also save the configuration to a file. For instructions on how to do this with Configuration Manager, refer to the documentation for your unit.

- 2 Restart the RLC.
-

What's next?

Now that you have configured the minimum information required for network connectivity, perform the following tasks:

- test the network connections.
For instructions, refer to “Testing the connections” on page 96.
- perform additional configuration, if needed.
For instructions, refer to Chapter 6, “Configuring the RLC”.

Testing the connections

Use the following methods to test the connections to the RLC:

1. Check your system's host-site connections to ensure basic PSTN and IP Network connectivity.
2. Perform a PING test. To perform this test, the following must be true:
 - The RLC must be physically connected to the IP network.
 - A link LED must be on.
 - You must be physically connected to the network.
 - You must be logged on to Configuration Manager.

Check host site connections

When testing the connections in your remote services network, you must first confirm that the equipment is connected properly at the host site.

Telephone network connections

Check the following points in your telephone network connection:

- Confirm that the proper connections are made for the digital telephones at the cross-connect system in your corporate switch room.
- Confirm that the RJ11 plug of the telephone wire leading to the digital telephone is properly and securely seated in the RJ11 jack in the wall.
- Confirm that the RJ11 plug at the other end of the telephone wire is properly and securely seated in the RJ11 jack at the base of the digital telephone.

If you are using the RLC Multi-I/O cable—Enhanced, check the following points, in addition to the items listed above:

- Confirm that the 25-pair connector of Plug 5 and the 25-pair connector of a cable leading to your cross-connect are properly and securely joined.
- Confirm that the 25-pair connector at the other end of the cable mentioned in the previous step is properly and securely joined to the 25-pair socket of the cross-connect.

- Confirm that the cable leading from the RLC to the cross-connect is in good condition, end-to-end.

Ethernet connection

Check the following points in your Ethernet connection:

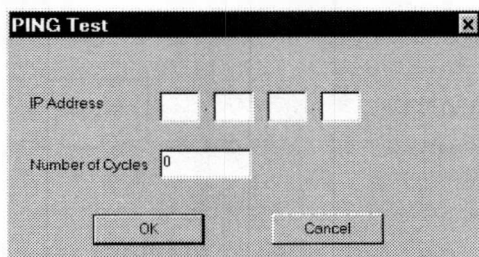
- Confirm that the DB15–RJ45 adapter at Plug 2 of the RLC Multi-I/O cable–Enhanced is properly and securely joined to Plug 2.
- Confirm that the RJ45 plug of a CAT5 data cable leading to your Ethernet hub is properly and securely seated in the RJ45 socket of the DB15–RJ45 adapter mentioned in the previous step.
- Confirm that the other end of the CAT5 data cable mentioned in the previous step is properly and securely seated in the appropriate Ethernet hub socket.
- Confirm that the CAT5 data cable leading to your Ethernet network's data router is properly and securely seated in the appropriate Ethernet hub socket.
- Confirm that the CAT5 data cable leading from your Ethernet hub is properly and securely seated in the appropriate socket of the data router mentioned in the previous step.

Performing a Configuration Manager PING

To perform a Configuration Manager PING:

- 1 From the menu, choose Tests → Ping.

Result: The PING Test dialog box appears.



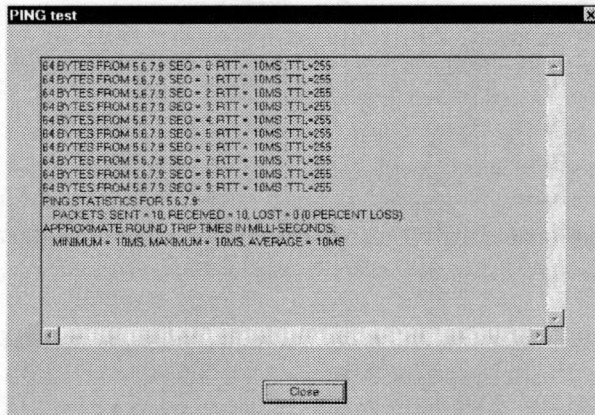
- 2 Enter the IP Address of the unit you want to ping.

- 3 In the Number of Cycles field, enter the number of times you want to ping the unit.

Note: The number must be in the range of 1 to 100.

- 4 Click on the **OK** button.

Result: The PING test results screen appears, showing the PING results. The following is an example of a successful PING.



- 5 Click on the **Close** button.

Result: The PING test screen closes.

Unsuccessful PING options

If the PING was unsuccessful:

- 1 Ensure you have entered the IP address, subnet mask, and default gateway correctly.
- 2 PING the gateway to see if it responds.
- 3 Contact your data network administrator if the PING still does not work.

What's next?

Once you have confirmed that the RLC can be recognized on the network, you can begin to configure it. Nortel Networks recommends that you also change the passwords for logging on to both Configuration Manager and the RLC.

For a description of Configuration Manager, refer to "What is Configuration Manager?" on page 120. To change passwords, refer to "Changing the administration password" on page 198.

Chapter 4

Configuring the host PBX for the RLC

In this chapter

Configuring the host trunk for a Remote Office 9150 unit	102
Configuring an RLC slot	104
Understanding port relationships	105
Configuring remote and network ports	106

Configuring the host trunk for a Remote Office 9150 unit

Remote Office 9150 units require an end-to-end digital connection. Tell your service provider which type of ISDN connection (PRI or BRI) that you need for your remote service equipment. Nortel Networks recommends ISDN PRI trunks for connecting the CO to the host PBX. Tell your service provider the parameters to configure on the trunk according to the features that you want on the devices at your remote location. For more information on Remote Office trunk configuration, refer to the *Remote Office Network Engineering Guidelines* (NTP 555-8421-103). To locate this document, click on the Customer Support, Documentation, and North America links at the following website:

www.nortelnetworks.com

ISDN PRI configuration

ISDN PRI trunks transport Remote Office 9150 unit calls between the host PBX and the PSTN. To ensure full functionality for all remote sites served by each RLC, ask your service provider to configure the following elements on each trunk:

- two-way voice and two-way data capability
- caller ID
- end-to-end digital circuitry, no analog segments (confirm this with both long-distance and local service providers)
- non-blocking configuration (ensure that configuration will not block remote site traffic)
- 56K or 64K clear channel, according to your equipment

ISDN BRI configuration

Some locations require ISDN BRI service from the host PBX (the host trunk connection) instead of PRI for geographical reasons. ISDN BRI configuration is identical to ISDN PRI configuration. Verify this with your service provider. For information about ordering BRI service, refer to the *Remote Office Network Engineering Guidelines* (NTP 555-8421-103). For information on how to obtain this document, refer to “Related information products” on page xxii.

Note: In North America, an ISDN BRI line can only be ordered as a subscriber line and is not a valid trunk option.

Configuring an RLC slot

For the host PBX to communicate properly with RLCs, you must configure each RLC slot as an Extended Digital Line Card (XDLC) slot. Refer to the documentation for your PBX to complete this procedure.

Understanding port relationships

This section focuses on the relationship between the two principle RLC ports in a system using the PSTN:

- remote ports
- network ports

ATTENTION

This section is critical to your understanding the operation of the Reach Line Card.

Functionality provided by the various port types

You can configure ports on the RLC as one of the following:

- a remote port
Remote ports support digital telephones on remote units for host-controlled calls. The PBX features and DN's assigned to the RLC ports are the PBX features and DN's available to the remote telephones.
- a network port
Network ports place and receive PSTN calls to and from remote devices. Network ports require only the most basic configuration on the host PBX that allows this port to place and receive calls of the appropriate type for the particular remote unit. RLC network ports do not use PBX features such as conference or call forward.
When Quality of Service on the IP network degrades, QoS Transitioning Technology opens PSTN connections using paths provided by the network ports. Refer to "Configuring Quality of Service" on page 182 for information on configuring QoS thresholds.
- a local TCM port
Local TCM ports support local telephones connected at the host PBX.

Configuring remote and network ports

Observe the following rules when configuring remote and network ports for Remote Office systems.

General

Basic Remote Office configuration starts with the guidelines listed in this section.

- Configure one remote port for each remote device, such as a digital telephone or a fax machine, that you want the RLC to support.
- Configure at least one network port for each Remote Office unit that you want to support with the RLC.

Note: Each network port provides up to 64K of PSTN bandwidth between the RLC and the Remote Office 9150 unit. To provide 256K of bandwidth between the RLC and a Remote Office 9150 unit, configure four network ports. For the specific procedure to configure remote and network ports, refer to the documentation for your PBX.

At your PBX administration terminal, configure voice ports to the appropriate RLC remote ports supporting remote digital sets using any of the following:

- Remote Office 9150 units
- Remote Office 911x units
- Meridian Digital Telephone Internal IP Adapters
- Meridian Digital Telephone External IP Adapter
- Analog Telephone Adapters (ATAs)

Note: Remote Office 911x units do not support ATAs.

RLCs

One 16-port RLC supports a maximum of four Remote Office 9150 units, 16 Remote Office 911x series units, or 16 Meridian Digital Telephone IP Adapter units.

One 32-port RLC supports a maximum of four Remote Office 9150 units, 20 Remote Office 911x series units, or 20 Meridian Digital Telephone IP Adapter units.

Remote Office 9150 units

Every port on a single Remote Office 9150 unit must be served by the same RLC.

Remote Office 911x series units and Meridian Digital Telephone IP Adapter units

Associate every Remote Office 911x unit or Meridian Digital Telephone IP Adapter unit with one port on an RLC.

Refer to your PBX documentation for the exact procedures and a complete list of possible settings for voice and data ports.

Remote port configuration

Configure each remote port on the host PBX according to the device connected to it at the remote site. If that device is a telephone, configure the port with all the features (for example, voice mail and call transfer) that you want.

- On the host PBX, configure ports for all remote service digital telephones as voice ports.
- On the host PBX, configure ports for all remote service MCA data adapters supported by the RLC as data ports (Remote Office 9150 units only).
- If you have enough data ports available on your Remote Office 9150 unit, configure ATA data adapters supported by the RLC as data ports on the host PBX. If you do not have enough data ports available, you can set up ATAs on voice ports on the host PBX.

Note: Remote Office 911x series units do not support data adapters.

Fax relay support

You can use the following compression algorithms for fax transmission:

- **G.711**
If you select G.711, then faxes are transmitted at 64 Kbps. In this mode, the fax protocol is not interpreted. Therefore, all non-standard fax features are supported regardless of the manufacturer.
- **G.729/Fax**
If you select G.729/Fax, then the fax protocol is interpreted, and the fax modem is demodulated in an attempt to reduce the amount of bandwidth that is consumed. In this mode, the fax transmission is restricted automatically to 9.6 Kbps. The G.729/Fax algorithm provides more bandwidth efficiency at the expense of greater protocol-sensitivity and potentially lower fax speeds.

Note: Error Correction Mode (ECM) is automatically disabled during fax relay.

Configuration for fax relay support

On the host PBX, you must configure the TN associated with any remote analog ports (ATA or the Remote Office 9150 unit analog port) as a voice port.

Do this by ensuring that the remote ATA devices, or the Remote Office analog port, map to an ATA port on the RLC. ATA ports were introduced in Release 22 of Meridian system software. The ATA appears in the data port range, but the class of service treats the TN as a voice TN.

You can map remote analog ports (that appear in the voice port range on any supported release of Meridian software) to non-ATA voice ports on the RLC.

PBX

Configure the host PBX as follows:

- 1** Program the data TN for a digital set.
 - a. If you have a telephone programmed against the voice TN, then the data TN telephone type must be the same as the voice TN telephone type. For example, if the telephone on voice TN 6 15 is a 2616 then the fax data TN 6 31 should be programmed as 2616.
 - b. Set DTAO = MCA
 - c. Set the DN of the fax machine or ATA on Key 0 of the data TN.

- 2 After programming the data TN, go back in again to change the CLS. Do one of the following:
 - If the system software includes package 186, program an ATA by adding CLS=FLXA VCE CPTD.
 - If you do not have package 186 then, add CLS =FLXA VCE.
- 3 Enable the TN in LD 32.

RLC

Configure the corresponding ports on the RLC as follows:

- 1 Access Configuration Manager → RLC → RLC Port Configuration.
- 2 On the RLC port that matches the ATA port, configure the compression, priority and usage. This port should also be configured as a remote port, not a network port.
- 3 Click on the **OK** button on the RLC Port Configuration window, send to unit, save configuration to Flash and reboot the unit.

Note: When you save configuration changes to Flash, the system suspends new call processing for approximately 30 seconds.

Note: If you intended to use a fax on the ATA device, or you are programming the 9150 fax port, the G.729/Fax compression is recommended.

Remote Office 9150 unit

Configure the Remote Office 9150 unit as follows:

- 1 For the Remote Office 9150 fax port, do the following:
 - a. Access Configuration Manager → 9150 → 9150 Port Configuration.
 - b. Map port 64 on the Remote Office 9150 unit to the data port on the RLC.
 - c. For an ATA adapter, map the 9150 port that is 16 ports above the telephone that house the ATA adapter. For example, if the telephone housing the ATA is on the Remote Office 9150 unit and is wired to port 0, then the ATA is configured on the Remote Office 9150 unit port 16).
 - d. Map the ATA port to the RLC data port configured on the host PBX.
- 2 Verify that any other unused Remote Office 9150 port that has the same RLC port number as the Fax or ATA is configured as Local.

For example, if the RLC data port 31 (mapped to 9150 port 64) is being used for fax, make sure the Remote Office 9150 unit port 31 is set to local only. This prevents any possibility of port contention occurring at the host side.

Also, make sure that the telephone type for the ATA port is selected as ATA not as a digital set.

- 3 For LOCAL 9150 access only from the Remote Office 9150 unit, configure the ATA port Local Call Key1 to Key Number 0.
- 4 If the port is configured for local and remote, verify that Forward Busy/No Answer is disabled.
- 5 Click on the **OK** button on the 9150 Port Configuration window, then click on the **Send** button.
- 6 From the Upload/Download menu option, select Save to Flash.

Note: When you save configuration changes to Flash, the system suspends new call processing for approximately 30 seconds.

- 7 Reboot the unit.

Network port configuration

Configure the RLC network ports that are connected to Remote Office 9150 units as MCA data adapters with the first line able to place and receive data calls. Configure the 911x network ports on the RLC as voice ports with flexible voice/data allowed. To configure data ports, refer to “Sample configuration files” on page 299.

- If the RLC and its remote units connect only through the IP network, you do not need to configure network ports for the RLC. The RLC and remote units use an IP path to communicate with one another.
- If your system uses both the IP and PSTN connections to route calls, configure a sufficient number of network ports for the RLC to handle the anticipated traffic between the remote units and the host PBX.
- If you are configuring a Remote Office 911x series unit, only the Remote Office 9115 module supports Meridian Communication Adapters (MCAs). Remote Office 9115 units support MCAs only to allow CTI control of the digital telephone when operating in transparent mode.
- Remote Office 911x series units do not support Analog Telephone Adapters (ATAs).

For further details, refer to the section on LD 11 in the *Meridian 1 X11 I/O Guide* (NTP 553-3001-400).

Meridian 1 network port configuration for a Remote Office 9150 unit

To support a Remote Office 9150 unit on a Meridian 1, you must configure the RLC network port as follows:

- Class of Service: DTA, FLXD
- DTAO prompt must be configured as MCA
- BRI CLS should include: VCE DTA
- TSP should set: USID = 0

Note: For MSL-100, similar configuration rules apply. For configuration requirements, refer to “MSL-100 configuration requirements” on page 113.

Meridian 1 network port configuration for a Remote Office 911x series unit

To support a Remote Office 911x series unit on a Meridian 1, you must configure the RLC network port using the same procedure as described for PBX configuration for ATA. Refer to “PBX” on page 108 for details.

Note: For MSL-100, similar configuration rules apply. For configuration requirements, refer to “MSL-100 configuration requirements” on page 113.

RLC and Remote Office 9150 unit connection paths

The RLC network ports (used to connect to the Remote Office 9150 units) carry HDLC-framed data. You must configure these ports so that they can transparently pass this data.

Any port you configure as a data port on the Meridian 1 can be an RLC network port.

If the Meridian 1, instead of a PSTN or PTT, provides the Remote Office 9150 unit's ISDN number, you must configure the line on the host PBX (LD 27 on the Meridian 1) as follows:

- 1 Set B1CT to VCE and DTA.
- 2 Set B2CT to VCE and DTA.
- 3 Set USID to 0.

PBX trunks and RLC network ports

When using the Remote Office unit with PSTN connectivity, the PBX trunks must provide data capability. To make sure that the PBX is ready for data calls, complete the following outlined checkpoints:

- 1 Use the PRT command in LD20 on the PBX to print out the Network Port TNs that have been provisioned against the RLC slot. Make note of the TGAR and NCOS values.

Note: For specific printing instructions, refer to your PBX documentation.

- 2 Print out the PBX Route Data Block (RDB) in LD 21. For each PRI:
 - a. Review the TARG values. If the values match the Network Port TGAR, calls are NOT allowed through the PRI.
 - b. Review the trunk capability at the DSEL prompt. It should be "Voice or Data" (VOD) or "Data Only" (DTA).
 - c. Check that the ICOG prompt is Incoming and Outgoing (IAO).

Note: If you make changes to the DSEL, or the ICOG prompt, make sure that the central office is configured likewise, that is to say, changing the DSEL from VCE to VOD can be ineffective because the CO still rejects data calls.

- 3 Print out the PBX trunk time slot configuration information in LD 22 CEQU. Ensure that there are an adequate number of time slots provisioned with data capability. Here is an example of the printout:

(data omitted)

```

DLOP NUM DCH FRM LCMT YALM TRSH
TRK 001 24 D4 AMI DG2 00 <-- DTI trunks
    012 24 D4 AMI DG2 00
PRI 003 24 ESF B8S FDL 00 <-- PRI trunks - voice or data
    051 00 ESF B8S FDL 00
  
```

A DCH setting of 0 indicates that 0 time slots are usable for data call capability. You should have 24 by default.

Note: The above example displays the North American default values.

- 4 If the RLC is dialing to the Remote Office unit, and the number being dialed is using the PBX routing (for example, 9 or 6 access code), you need to make sure that the call is presented to the PRI trunk and not a standard CO trunk.

Verify that the Network Port TN NCOS has the capability to access the PRI. One way to ensure that the PRI is accessed is to use the Trunk Access code (ACOD) which was printed in step 2.

You can modify the RLC Remote Connection PSTN information to use the ACOD to directly access the trunk. For example, set the Remote Connection number to be #8002#5551212, assuming that 8002 is the trunk ACOD and you are placing a local call.

How the remote and network ports work together

RLCs configured as PSTN-only, or in QoS transition situations, route voice traffic through the PSTN. a call placed to voice port 0 can be relayed to a Remote Office 9150 unit configured as PSTN-only. For this call, the RLC calls the Remote Office 9150 unit using the dedicated network port for that unit. Each network port on a Remote Office 9150 unit supports up to eight simultaneous calls using G.729 (8 Kbps) compression. For Remote Office 911x units, each network port supports only one call, regardless of compression.

MSL-100 configuration requirements

This section describes the MSL-100 PBX configuration that is needed to support the Remote Office 9150 unit.

Note: You must configure the Meridian unit operating behind an MSL-100 PBX using Meridian 1 key numbering.

M2000 telephone set key numbering

The key numbering convention for M2000 series telephones on the Remote Office 9150 unit is different from the key numbering convention on the MSL-100 PBX.

On the Remote Office 9150 unit, keys are numbered from 0 through 15, whereas on the MSL-100 PBX, keys are numbered from 1 through 16. Refer to the following figure for a comparison:

M2616				
15	16	—	8	7
14	15	—	7	6
13	14	—	6	5
12	13	—	5	4
11	12	—	4	3
10	11	—	3	2
9	10	—	2	1
8	9	—	1	0
<u>M1</u>	<u>MSL-100</u>	<u>MSL-100</u>	<u>MSL-100</u>	<u>M1</u>

M0200 option on telephone set

M0200 must be assigned to the M2616 telephone set configuration on the MSL-100 PBX. Without this option, the M2616 telephone set does not function properly.

Port configuration

The port numbering on the RLC is different from the port numbering on the MSL-100 PBX. Refer to “RLC and MSL-100 port numbering comparison” below.

RLC and MSL-100 port numbering comparison

Port type	RLC port numbering	MSL-100 port numbering
Voice ports	0–15 and 32–47	Even-numbered ports
Data ports	16–31 and 48–63	Odd-numbered ports

RLC and MSL-100 port mapping

The following table identifies the port mapping between the RLC and the MSL-100:

16-port RLC				32-port RLC			
RLC voice ports	IPE voice ports	RLC data ports	IPE data ports	RLC voice ports	IPE voice ports	RLC data ports	IPE data ports
0	0	16	1	32	0	48	1
1	2	17	3	33	2	49	3
2	4	18	5	34	4	50	5
3	6	19	7	35	6	51	7
4	8	20	9	36	8	52	9
5	10	21	11	37	10	53	11
6	12	22	13	38	12	54	13
7	14	23	15	39	14	55	15
8	16	24	17	40	16	56	17
9	18	25	19	41	18	57	19
10	20	26	21	42	20	58	21
11	22	27	23	43	22	59	23
12	24	28	25	44	24	60	25
13	26	29	27	45	26	61	27
14	28	30	29	46	28	62	29
15	30	31	31	47	30	63	31

Sample datafill for network ports

For ISDN BRI connectivity and QoS transitioning functionality, each 64 Kbps trunk requires a dedicated data port on the RLC. On the MSL-100, you must configure this data port as a Meridian Communications Adapter (MCA) and datafill it as a 64K synchronous adapter. The following is an example of the SERVORD command used to provision a synchronous MCA adapter:

```
NEW $ 2386152 MCA MTL1 0 12 214 Y MCA N S 64000 I N N N N N N 0
HAYES $ HOST 20 2 01 03 $
```

```
>QLEN 2386152
```

```
LEN:      HOST 20 2 01 03
```

```
TYPE: SINGLE PARTY LINE
```

```
SNPA: 214
```

```
DIRECTORY NUMBER:      2386152
```

```
LINE CLASS CODE: MCA
```

```
CUSTGRP:      MTL1 SUBGRP: 0 NCOS: 12 RING: Y
```

```
DATA UNIT PROFILE:
```

```
CLASSDU: MCA      IDLETO: 0  DOWNLOAD: N
```

```
CONFIG: DTE      DTEIF: RS232C
```

```
SYNCHRO: S  DATARATE: 64000  CLOCKSRC: I
```

```
DUPLEX: F      KBDTYP: HAYES
```

```
HOTLINE: N  VLL: N  V.25: N  HDLC: N  RTS: N
```

```
DPOPTS:
```

```
CARDCODE: DR68AA GND: N  PADGRP: NPDGP  BNV: NL MNO: Y
```

```
PM NODE NUMBER      :      105
```

```
PM TERMINAL NUMBER :      36
```

```
OPTIONS: NDC
```

```
KEY      FEATURE
```

```
NONE
```

M39xx Release 2 telephones with MCAs

When configuring RLCs for Quality of Service (QoS) transition, you must configure a data port as a Meridian Communications Adapter (MCA).

A patch is required for MSL-100 sites using only M39xx Release 2 telephones and PBX software versions MSL14 or earlier to allow QoS transition. This is due to the fact that MSL-100 PBXs using software version MSL14 or earlier and configured for only M39xx Release 2 telephones do not recognize MCAs.

The patch numbers are:

- JDT01.xxx
- JDT04.xxx

where xxx denotes the PBX version number.

Contact your Nortel Networks distributor to receive the patch.

Chapter 5

Using Configuration Manager

In this chapter

What is Configuration Manager?	120
Starting and viewing Configuration Manager	121
Configuration files description	125
Working with configuration files	132
Selecting the device type for offline configuration	135
Logging on to a unit	136
Logging off of the unit	142
Performing a system restart or shutdown	143
Closing Configuration Manager	145

What is Configuration Manager?

Configuration Manager is a Windows-based software application that you install on your PC. Configuration Manager allows you to configure, administer, and upgrade the RLC. These tasks can be performed over either of the following connection types:

- 10BaseT Ethernet
- RS-232 serial

The CD shipped in the RLC package includes the Configuration Manager software. You can obtain the CD from your Nortel Networks distributor or click on the Customer Support and Software Distribution links at the following website:

www.nortelnetworks.com

Windows PC requirements

For the required characteristics of the Meridian administration PC, refer to “Windows PC requirements” on page 62.

Installing Configuration Manager

To install the Configuration Manager software on your administration PC, refer to “Configuration Manager software installation” on page 82.

Updating Configuration Manager

To update the Configuration Manager software, click on the Customer Support and Software Distribution links at the following website:

www.nortelnetworks.com

Save the software to the local hard drive on your administration PC.

To complete the installation, refer to “Configuration Manager software installation” on page 82.

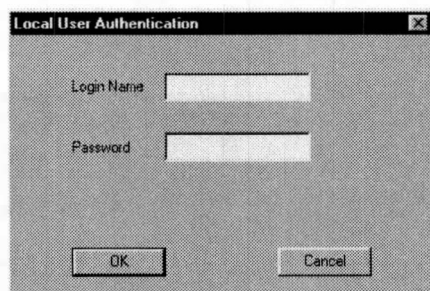
Starting and viewing Configuration Manager

The Configuration Manager software application is best viewed when your monitor settings are configured as 1024 by 768 pixels using Small Fonts at 96 dpi. If you use larger fonts, some fields and buttons might be hidden. You must use the horizontal and vertical scroll bars to view the hidden fields or buttons. For instructions on changing your display settings, refer to the Windows online help on your PC.

To start and log on to a Configuration Manager session:

- 1 From the Menu Bar, choose Start → Programs → Remote Office → Configuration Manager.

Result: Configuration Manager opens and prompts you for the logon name and password.



- 2 Enter **admin** in the Login Name box.
- 3 Enter **root** in the Password box.

Note: This is the default password. You can change the password after installation, though Nortel Networks recommends that you do not change the password until your Remote Office system is up and running.

- 4 Click on the **OK** button.

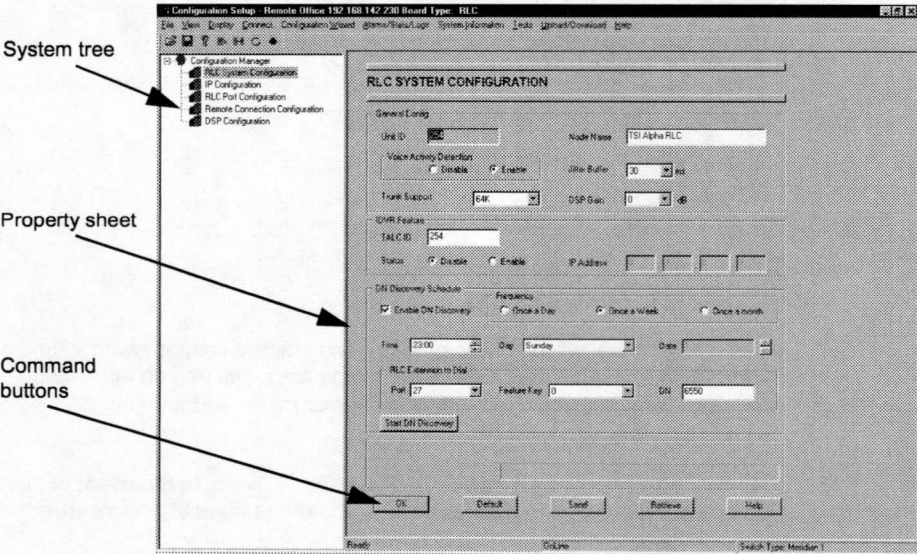
Result: The system informs you of a successful logon. In the event of an unsuccessful logon, the system informs you of the need to re-enter the information.

- 5 Click on the **OK** button.
Result: The logon status dialog box disappears.
- 6 Proceed as follows:

To perform an	Refer to
online configuration	"Logging on to a unit" on page 136.
offline configuration	"Selecting the device type for offline configuration" on page 135.

System tree

The left pane of Configuration Manager lists the property sheets you can access. To expand the list of all the property sheets associated with the logged-on or selected remote device, click on the plus (+) sign. (To hide the list, click on the minus (-) sign.) With the System Tree expanded, click on a configuration to display the associated property sheet in the right pane, similar to the following:



To hide the system tree, choose View → Tree Bar from the Menu Bar. The screen redraws itself showing only the right pane and displaying the selected property sheet. To display the system tree again, choose View → Tree Bar.

Property sheets

When you are logged on to a particular Remote Office node (that is, a Remote Office 911x series unit, a Meridian Digital Telephone IP Adapter unit, a Remote Office 9150 unit, or an RLC), Configuration Manager displays a system tree specific to the logged-on unit.

Note: When working with a Meridian Digital Telephone IP Adapter unit in Configuration Manager, use Remote Office 911x property sheets.

When you click an item in the system tree, the associated property sheet appears in the right pane. For instructions on selecting a device type when not logged on, refer to “Selecting the device type for offline configuration” on page 135.

Command buttons

The following buttons appear on every property sheet listed in the first level of the Remote Office Configuration Manager system tree (left pane):

- **OK**
Click on this button to accept any changes you have made to the displayed property sheet. This command stores these values in a temporary file on your PC until you are ready to update the unit's Flash memory. For more details, refer to “OK” on page 127.
- **Default**
Click on this button to insert default values into every field in the displayed property sheet.
- **Send**
Click on this button to update the buffer of the unit you are logged on to with the values currently on the displayed property sheet. For more details, refer to “Send” on page 128.

- **Retrieve**

Click on this button to display the saved configuration value for every field on the displayed property sheet from the unit's local buffer, containing the last sent data. For more details, refer to "Retrieve" on page 129.

- **Help**

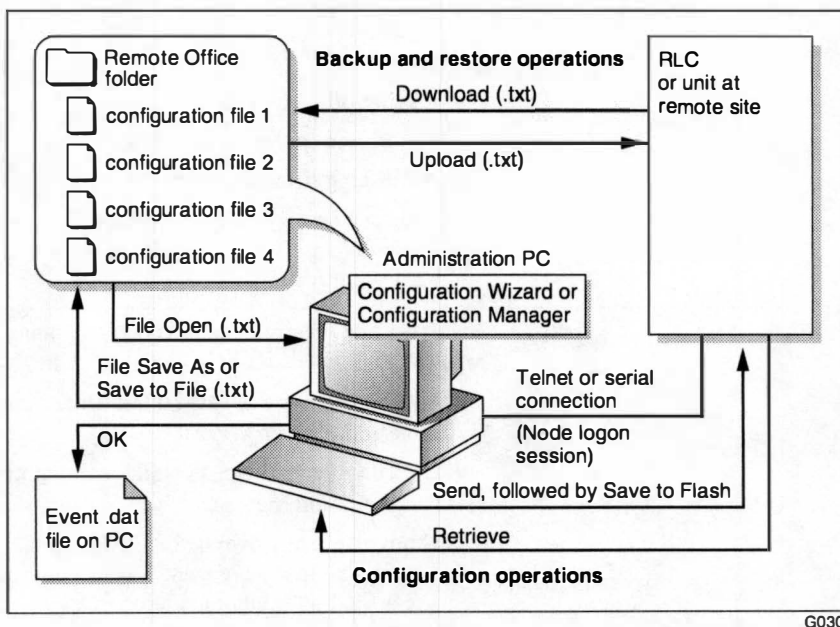
Click on this button to view online Help for the displayed property sheet.

Configuration files description

This section describes configuration files and the ways that you can work with them.

Configuration Manager: file operations diagram

The following diagram shows how configuration information is stored. A detailed description of each file type and operation follows.



Types of files

You can work with three types of files in Configuration Manager. Each file is identified by one of the file name extensions described in the following table.

File name	File type	When it is created and used
■ event.dat	Log file	The log (event.dat) file records all activities (and messages associated with those activities) that you perform while running Configuration Manager, such as: ■ logging on to Configuration Manager ■ logging on to a unit (by serial or Telnet connection) ■ logging off from a unit ■ performing configuration changes ■ performing firmware upgrades This file can be very useful when troubleshooting system problems. Technical support personnel may ask for this file.
■ *.txt	Text	The text (.txt) file is created when you do one of the following: ■ click on the Save to File button while running the Configuration Wizard. ■ click on File → Save As while working in Configuration Manager. ■ choose Upload/Download → Download Configuration to save a unit's configuration in a text file on the administration PC.
■ *.upg	Upgrade	Use the upgrade (.upg) file when performing firmware upgrades. For more details, refer to "Performing a firmware upgrade" on page 248.

Configuration Manager: file operations description

The following table describes each operation shown in the “Configuration Manager: file operations diagram” on page 125.

Operation	Description
OK	When you click on the OK button, the following occurs: ■ Configuration Manager checks any changes you made for errors that, if found, produce an error dialog box. Make the necessary changes, and then click on the OK button again. Note: You must click on the OK button after making changes to a property sheet. For Configuration Manager to be able to save your information, you must first click on the OK button to accept the changes. After clicking on the OK button, you can send the changes to the logged on unit's buffer using a Send or Send All command. You can now update the Flash memory of the logged on unit by performing an Upload/Download → Save to Flash operation from the Menu Bar. For more details, refer to “Send” on page 128. Note: If you do not click on the OK button on a property sheet before displaying another property sheet, you lose all of the changes made on the first property sheet. To regain lost changes, you must reenter them.
File → Open	When you choose File → Open from the Menu Bar, you can open a previously saved configuration file. This is useful for preparing and storing configuration files in a central location before they are deployed to remote locations in the network. Note: To open a file, the file type must be text (.txt).

Operation	Description
File → Save As	When you choose File → Save As from the Menu Bar, Configuration Manager saves the unit's configuration to a file on your PC. You must specify the file name and directory location. After saving the file, you can open and modify it at a later time. Notes: ■ Configuration Manager saves the file as a text (.txt) file. ■ If you close Configuration Manager without choosing File → Save As, you lose all of the changes you made.
Send	When you click on the Send button, Configuration Manager sends any changes made on the displayed property sheet to the buffer of the logged-on unit. If the send is successful, the following message displays: Data Sent Successfully (It is recommended that you click on the OK button before clicking on the Send button.) Note: You must choose Upload/Download → Save to Flash from the Menu Bar to save the changes to the unit's Flash memory. For more details, refer to "Save to Flash" on page 129.
Send All	When you choose Upload/Download → Send All on any property sheet, changes for <i>all</i> property sheets pertaining to the logged-on unit are sent to the buffer on the unit you are connected to. If the send is successful, the following message displays: Data Sent Successfully Note: You must choose Upload/Download → Save to Flash from the Menu Bar to save the changes to the unit's Flash memory. For more details, refer to "Save to Flash" on page 129.

Operation	Description
Retrieve	When you click Retrieve on a property sheet, the configuration stored in the buffer of the unit that you are connected to (the latest configuration information) displays in Configuration Manager. If the retrieval is successful, the following message displays: Data Received Successfully
Save to Flash	When you choose Upload/Download → Save to Flash from the Menu Bar, the information stored in the logged-on unit's buffer is saved to Flash memory. This prevents the configuration from being lost if the unit loses power. While in progress, the following message displays in the status bar at the bottom of the screen: Save to Flash When the Save to Flash is completed, the Data Stored to Flash dialog box displays. Some changes require a restart of the unit after saving the changes. If a restart is necessary, Configuration Manager prompts you to do so. Notes: ■ You must click on the Send button or choose Upload/Download → Send All from the Menu Bar <i>before</i> you choose Upload/Download → Save to Flash. You should perform a Save to Flash as often as you think it is necessary, to keep your configuration information safe. ■ Do not ignore error messages in the Save to Flash process. If Save to Flash fails, retry uploading and saving to Flash. If the problem persists, check the file being uploaded and report the problem to Nortel Networks.

Operation	Description
Upload Configuration	When you choose Upload/Download → Upload Configuration from the Menu Bar, Configuration Manager uploads the configuration file you specify and writes the file to the buffer on the logged-on unit. Use this option if you need to restore or replace an entire configuration. You must choose Upload/Download → Save to Flash from the Menu Bar to save the changes in the unit's flash memory. If you do not perform the Save to Flash and a power loss occurs on the unit, you lose the changes. While in progress, the following message displays in the status bar at the bottom of the screen. Save to Flash in Progress When the Save to Flash is completed, the Data Stored to Flash dialog box displays. Notes: ■ To upload a configuration file, the file type must be text (.txt). ■ To perform a configuration upload over the IP network, a TFTP server application must be running on your PC. Uploads over the serial port are not supported. ■ Restart the unit after the Save to Flash operation. For instructions on how to restart the unit, refer to "Performing a system restart or shutdown" on page 143. ■ If the upload fails or aborts, confirm that you are uploading the correct file. If the problem persists, contact Nortel technical support for assistance.

Operation	Description
Download Configuration	When you choose Upload/Download → Download Configuration from the Menu Bar, Configuration Manager saves the configuration stored on the logged-on unit to a file on the PC. Use this option if you want to create a backup of the unit's configuration. Notes: ■ The downloaded file is saved as a text file (.txt). ■ If you make changes and do not save them, you lose those changes.

Working with configuration files

This section explains how to:

- create a configuration file (refer to page 133)
- open a configuration file in Configuration Manager (refer to page 133)
- perform a configuration upload (refer to page 134)
- perform a configuration download (refer to page 134)

When to use Configuration Manager file operations

You can use	When you are
OK, File → Open, and File → Save As	working in offline mode or connected and logged on to a unit. Note: When working in offline mode, you must save the configuration to a file. However, when you are logged on to a unit, the file save operation is optional. To save the configuration to Flash, first update the unit's local buffer by clicking on the Send button or choosing Upload/Download → Send All from the Menu Bar. Then, use Upload/Download → Save to Flash to complete the operation.
■ Send ■ Send All ■ Retrieve ■ Upload Configuration ■ Download Configuration	logged on to a unit.

Creating a configuration file on the PC

To create a configuration file on the PC:

- 1 Start Configuration Manager.
- 2 Make the required changes on each property sheet.

Note: You do not have to be logged on to a unit to make configuration changes. When you are not logged on to a unit, you can perform an *offline configuration*.

- 3 From the Menu Bar, choose File → Save As.

Result: The Save As dialog box displays.

- 4 Enter a descriptive name for the file.

The file name should identify the type of configuration it contains.

Example 1: If the file contains a basic configuration that is to be used for a specific type of unit, you can enter **template** as the file name.

Example 2: If the file contains a configuration that is unique to a specific unit, you can enter the unit's **name or number** as the file name.

- 5 Ensure that the Save as type drop down box shows text file (*.txt)
- 6 Specify the folder where you want to save the file.
- 7 Click on the **OK** button.

Result: The file is saved.

Note: Nortel strongly recommends that you do not manually edit this file.

Opening a configuration file

To open a configuration file:

- 1 Start Configuration Manager.
- 2 If you want to work in online mode, log on to the unit. Otherwise, ensure that you have selected the device type.
- 3 From the Menu Bar, choose File → Open.

Result: The Open dialog box displays.

- 4 Ensure the Files of type drop down box shows text files (*.txt).
- 5 Navigate to the folder containing the file you need.

- 6 Select the file, and then click on the **Open** button.
Result: The contents of the configuration file are loaded into Configuration Manager.
- 7 View the configuration details by clicking each item in the system tree to display the associated property sheet.
- 8 Make changes as necessary, then complete the following actions:
 - a. Save the file by choosing File → Save from the Menu Bar. If you want to change the file name, choose File → Save As from the Menu Bar.
 - b. Click on the **Send** button to update the unit, then choose Upload/Download → Save to Flash from the Menu Bar.

Uploading a configuration to a unit

For complete instructions on uploading a configuration to a unit, refer to “Restoring the configuration” on page 203.

Downloading a configuration from a unit

For complete instructions on downloading a configuration to a unit, refer to “Creating a backup configuration file” on page 200.

Selecting the device type for offline configuration

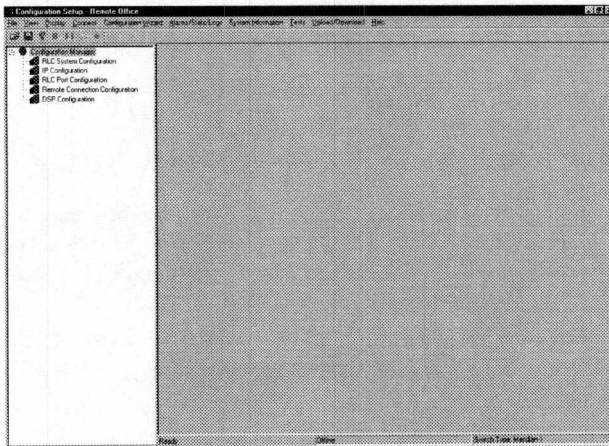
If you are not logged on to a Remote Office unit (that is, an RLC, Remote Office 9150 unit, a Remote Office 911x series unit, or a Meridian Digital Telephone IP Adapter unit), then you must select the device type you want to work with. Configuration Manager reorganizes the system tree with the property sheets associated with that device type.

Note: When working with a Meridian Digital Telephone IP Adapter unit in Configuration Manager, use Remote Office 911x property sheets.

To select the device type for offline configuration:

- 1 Start Configuration Manager as described under "What is Configuration Manager?" on page 120.
- 2 From the Menu Bar, choose View → Device Type, and the type of device (for example, RLC, 9150, 911x).
- 3 Click on the plus (+) sign beside Configuration Manager in the left pane.

Result: The system tree expands in the right pane, similar to the following:

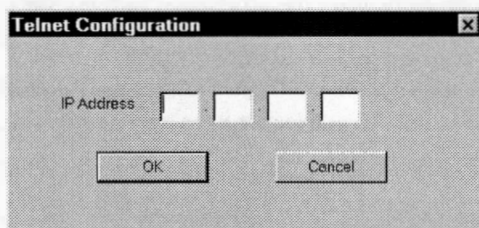


Logging on to a unit

To log on to a unit using Telnet:

- 1 From the Menu Bar, choose Connect → Logon Unit → Telnet.

Result: The Telnet Configuration dialog box displays, similar to the following:



- 2 Enter the IP Address of the unit you want to connect to.
- 3 Click on the **OK** button.

Result: If no one else logged on to the unit before you, and if IP connectivity exists to this unit, the User Authentication for Telnet Mode dialog box displays. It is similar to the User Authentication for Telnet Mode dialog box on page 137.

Default logon ID and password

The default logon ID is **guest**. You cannot change the logon ID.

The default password is **guest123**. The password can be changed and, therefore, can be different if this is not a first time installation. Nortel Networks recommends that you do not change the password until your Remote Office system is up and running smoothly.

Connection history

Configuration Manager maintains a record of past unit connections. You can select, and then connect to a unit from the history list that displays in the Connect menu.

Note: Upgrading the Configuration Manager software deletes the connection history list.

Auto logoff

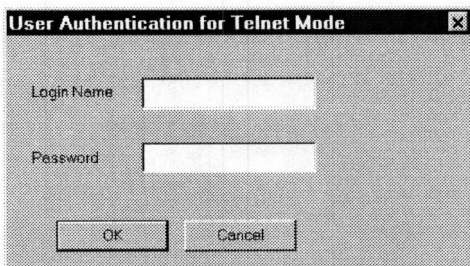
If the connection remains open with no activity for 15 minutes, then Configuration Manager automatically logs off the connection and the Session Timed Out message displays. This helps to secure the configuration in the event that you walk away from the administration PC while logged on to a unit.

Logging on to a unit using the connection history

To log on to a unit using the connection history:

- 1 From the Menu Bar, choose Connect → XXX.XXX.XXX.XXX (IP address of the unit you want to log on to).

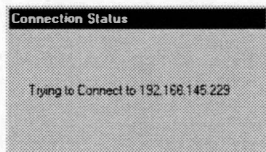
Result: If no one else logged on to the unit before you and if IP connectivity exists to this unit, the User Authentication for Telnet Mode dialog box displays. It is similar to the following:



- 2 Enter your logon name in the Login Name field. If you have not yet customized this setting, refer to "Default logon ID and password" on page 136 for the default logon ID.

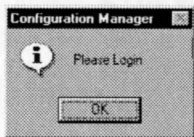
- 3 Enter your password in the Password field. If you have not yet customized this setting, refer to "Default logon ID and password" on page 136 for the default password.
- 4 Click on the **OK** button.

Result: Configuration Manager initiates a connection attempt. The Connection Status message box displays. It is similar to the following:



Note: The connection speed can be too fast for this message to be seen in a successful logon attempt.

If you do not enter any logon information, after two minutes Configuration Manager displays a reminder screen similar to the following:

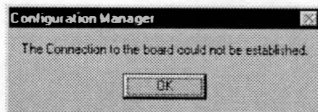


Click on the **OK** button to return to Step 2 on page 137.

IF the logon attempt THEN

fails,

a message box similar to the following displays:



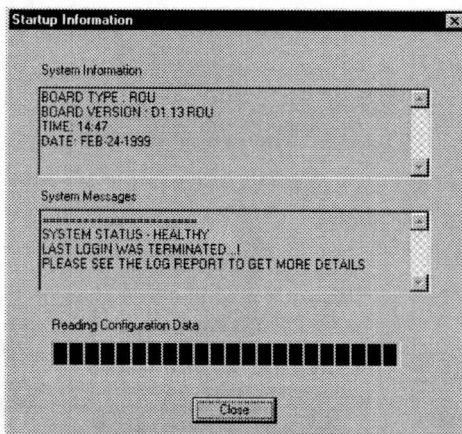
Complete the following actions:

- 1 Click on the **OK** button.
- 2 Go back to Step 1 on page 137 to try again.

IF the logon attempt THEN

succeeds,

the User Logged In dialog box displays.

Click on the **OK** button.**Result:** The Startup Information dialog box displays. It is similar to the following:

Messages appear above the progress bar at the bottom of the dialog box, similar to the following:

- Reading Hardware Information
- Reading DSP Load Data
- Reading Configuration Data

These messages mean that Configuration Manager is obtaining the unit's configuration information from Flash memory.

When initialization is complete, the Configuration Data Read Successfully message appears above the progress bar.

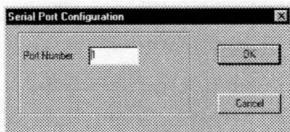
Click on the **Close** button.

Logging on to a unit using the serial port

To log on to a unit using the serial port:

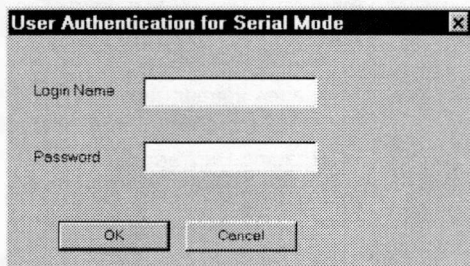
- 1 From the Menu Bar, choose Connect → Logon Unit → Serial.

Result: The Serial Port Configuration dialog box appears, similar to the following:



- 2 Enter the COM port number the unit is connected to in the Port Number field.
- 3 Click on the **OK** button.

Result: If no one else logged on to the unit before and if your PC is connected with a serial cable to the RLC, the User Authentication for Serial Mode dialog box displays. It is similar to the following:



- 4 Enter your login name in the Login Name field. Refer to "Default login ID and password" on page 136 for the default login ID if you have not yet customized this setting.
- 5 Enter your password in the Password field. Refer to "Default login ID and password" on page 136 for the default password if you have not yet customized this setting.
- 6 Click on the **OK** button.

Result: The connection attempt is initiated. The following message might display:

Trying to Connect via Serial Port <port number>

IF the logon attempt THEN

failed,

the following message displays:

SERIAL CONNECTION FAILED

Check the serial port connection and ensure it is good. Then, go back to step 1.

is successful,

the User Logged In dialog box displays.

Click on the **OK** button.

Result: The Startup Information dialog box displays.

Messages appear above the progress bar at the bottom of the dialog box, similar to the following:

- Reading Hardware Information
- Reading DSP Load Data
- Reading Configuration Data

These messages mean that Configuration Manager is obtaining the unit's configuration information from flash memory.

When initialization is complete, the Configuration Data Read Successfully message displays.

Click on the **Close** button.

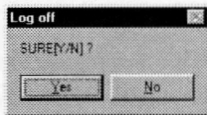
Logging off of the unit

When you are finished using Configuration Manager to make configuration changes, or to view logs and statistics, log off of the unit. Logging off secures the unit's configuration.

To log off of the unit:

- 1 From the menu, choose Connect → Logoff Unit.

Result: The Log off dialog box displays, similar to the following:



- 2 Click on the **Yes** button.

Result: The Configuration Manager: User Logged off dialog box displays, similar to the following:



- 3 Click on the **OK** button.

Performing a system restart or shutdown

Configuration Manager allows you to perform a controlled system restart or shutdown.

When to perform a restart or shutdown

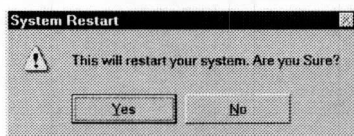
Configuration Manager informs you when you must perform a system restart. You can perform a shutdown when you need to power the system down.

Performing a system restart

To perform a system restart:

- 1 From the Menu Bar, choose Connect → System Reset → Restart.

Result: The System Restart dialog box displays, similar to the following:



- 2 Click on the **Yes** button.

Result: The status box displays.

The following message also displays in the status bar at the bottom of the screen:

Restarting the System

The status continues to show Online. When the system restart is complete, a dialog box displays informing you that the system restart was successful, and that you are logged off.

- 3 Click on the **OK** button.

Result: You are prompted to log back on using the previous connection method (Serial or Telnet).

Performing a system shutdown

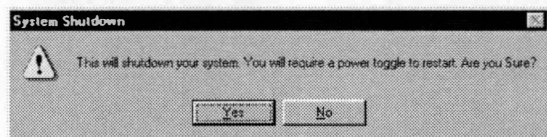
ATTENTION

Do not perform this procedure if you do not have physical access to the unit. To recover from the system shutdown, you must power off the unit, then turn it back on.

To perform a system shutdown:

- 1 Choose Connect → System Reset → Shutdown from the Menu Bar.

Result: The System Shutdown dialog box displays, similar to the following:



- 2 Click on the **Yes** button.

Result: Your logon session is disconnected, and the following message displays in the status bar at the bottom of the screen:

Shutting Down the System

The status shows Offline.

- 3 Turn the power on the Remote Office unit off.

Note: You must turn the power off before you can power the unit back up.

Closing Configuration Manager

When you have completed all of the configuration modifications you want to make, or are done viewing unit logs and statistics, log off and close the Configuration Manager application. This secures the configuration, preventing others from accessing it if you walk away from the administration PC while logged on to a unit. To close Configuration Manager:



CAUTION

Risk of configuration loss

If you close Configuration Manager without saving the changes you made to a file on your PC, or without updating the Flash memory of the unit you were working on, all changes are lost. You must reenter any changes you made.

- 1 Ensure that you have saved all configuration changes by doing one or more of the following:
 - From the Menu Bar, choose File → Save As, and then specify the name for the configuration file. The file is saved on the administration PC hard disk.
 - Update the Flash memory of the unit you are connected to, by doing one of the following:
 - Click on the **Send** button on any property sheet, then choose Upload/Download → Save to Flash from the Menu Bar.
 - Click on the **Send All** button on any property sheet, then choose Upload/Download → Save to Flash from the Menu Bar.
 - If you have saved the changes to a file, choose Upload/Download → Upload Configuration → Save to Flash from the Menu Bar. For instructions, refer to "Restoring the configuration" on page 203.
- 2 Log off by choosing Connect → Logoff Unit from the Menu Bar.
- 3 Choose File → Exit from the Menu Bar.

Result: Configuration Manager closes.

Chapter 6

Configuring the RLC

In this chapter

Using the XConnect command for PBX maintenance from a remote site	148
RLC system configuration	149
Understanding the IP interface	156
IP Configuration	158
RLC port configuration	162
Remote Connection Configuration	171
Configuring Quality of Service	182
How the online/offline table works	186
Online/Offline table configuration	189
Caller ID configuration	192
DSP configuration	194

Using the XConnect command for PBX maintenance from a remote site

This section shows you how to establish a connection to the host PBX's serial data interface (SDI) port from a remote site. First, you must ensure that there is a straight-through serial connection from the RLC to the PBX's SDI port. Then, you must log on to the RLC using Telnet. With these connections established, remote-site system administrators can perform PBX maintenance procedures.

Note: The terminal settings must be as follows: 9600 8 N 1 (9600 Baud, 8 data bits, No parity, 1 stop bit).

Getting there RLC → Configuration Manager

Connecting to the host PBX's SDI port from a remote site

To connect to the host PBX's SDI port from a remote site:

1 Log on to the RLC using Telnet.

2 Choose Connect → XConnect from the Menu Bar.

Result: Configuration Manager warns you that if you continue, you will be logged off the logged-on unit after you end your SDI session.

3 Click on the **Yes** button.

Result: Configuration Manager establishes the serial connection from the RLC to the host PBX's SDI port and presents you with the XConnect log screen.

4 Conduct the required PBX maintenance activities.

5 Click on the **Close** button to end your PBX configuration session.

Result: Configuration Manager closes the serial connection to the host PBX's SDI port and logs you off of the RLC.

RLC system configuration

There are three categories on the RLC system configuration property sheet:

1. **General Config**—Identify this RLC within your remote network and address voice quality and signal strength issues at the remote site. In addition, this category allows you to configure Trunk Support according to the speed of your connection.
2. **IDVR Feature**—The Integrated Digital Voice Recorder (IDVR) is a TelStrat Int'l product. For information on configuring IDVR functionality, contact your TelStrat Int'l representative.
3. **DN Discovery Schedule**—Set the times when the RLC automatically determines the name and number assigned to the all line keys on each RLC remote port.

Voice Activity Detection

Enable Voice Activity Detection (VAD) to prevent packet transmission during periods when there is no voice data present. This can help you to save bandwidth. To enable VAD, click on the **Enable** option button under Voice Activity Detection.

If you are having difficulties with voice quality, see if silence suppression has an effect on the problem by disabling VAD. To disable VAD, click on the **Disable** option button under Voice Activity Detection.

Note: When using the bandwidth rules described in the *Remote Office Network Engineering Guidelines* (NTP 555-8421-103), use the Peak Rate to calculate IP bandwidth overhead if VAD is disabled. Allocate additional bandwidth over the ISDN for PSTN connections between the RLC and the Remote Office 9150 unit, including QoS transition. When you enable VAD, the amount of bandwidth allocation is 120% of the normal rate. Therefore, if you use G.729, the bandwidth allocation is 9.6K instead of 8K. If you use G.726, the bandwidth allocation is 38.4K instead of 32K. If the available bandwidth over the PSTN is insufficient, the call is blocked and you receive a message indicating insufficient bandwidth.

Jitter Buffer target depth

The RLC's dynamic voice jitter attenuation buffer compensates for the uneven arrival of voice packets across data networks. This buffer collects packets that arrive unevenly and relays them evenly.

Select the size of the buffer in the Jitter Buffer drop down box. The valid options are 30, 60, and 90 milliseconds (ms).

Configure the jitter buffer according to the following guidelines when upgrading to Release 1.3:

- high-speed (>T1 connections) or LANs — leave at the default
- medium-speed (for example, fractional T1s with speeds of greater than 128K) — set to 60 milliseconds
- low-speed (64K or ISDN) or high-data environments — configure at 90 milliseconds. This is especially true if using G.711.

DN Discovery

Through DN Discovery, the RLC detects the PBX-configured name and number assigned to all line keys in its portion of the remote network.

Some of the characteristics of DN Discovery are:

- DN Discovery overrides the DN configuration for Local Call keys.
- Local SwitchOver and Bridge Ports require DN Discovery.
- The Remote Office 9150 unit also uses the discovered DNs to determine when it can switch calls locally.
- MADN appearances of the DN Discovery port ring periodically during DN Discovery. To avoid this, do not start DN Discovery more frequently than once per half-hour and add a unique SCR key for DN discovery.
- If Make Set Busy is active, DN Discovery fails and results in blank DN displays on M39xx sets. To avoid this, do not activate Make Set Busy for the port designated for DN Discovery.
- For DN Discovery to work using key 0 on the target port, no special Class of Service (CLS) is required. If the target key is key 1 or higher, TDD CLS is required.

- The target key must be an SCR or MCR key - not an ACD key.

DN Discovery configures the DNs for the local call keys based upon the first line key DN discovered in the PBX configuration of the RLC port. Therefore, the first line key DN must be unique on all sets.

How it works

At the configured time and day, or date, the RLC performs DN Discovery. It places a call from the first of its ports configured as “Remote” on the RLC Port Configuration property sheet. This call routes to the DN in the “RLC extension to dial: DN” field on the RLC System Configuration property sheet.

The host PBX regularly provides updated keymaps of the remote station's feature keys to the RLC. For each feature key configured as a line key, the RLC places a call. For each call, the host PBX produces Calling Line Identification (CLID) information revealing the primary DN of the remote port the call is placed to.

Getting there RLC → Configuration Manager → RLC System Configuration

RLC System Configuration property sheet

RLC SYSTEM CONFIGURATION			
General Config			
Unit ID	254	Node Name	TS1 Alpha RLC
Voice Activity Detection	☐ Disable ☒ Enable	jitter Buffer	30 ms
Traffic Support	54K	CSF Gain	0 dB
IPv4 Feature			
TALC ID	254		
Status	☒ Disable ☐ Enable	IP Address	
DN Discovery Schedule			
☒ Enable DN Discovery	Frequency	☐ Once a Day ☒ Once a Week ☐ Once a month	
Time	23:00	Day	Sunday
Date		Date	
RLC Extension to Dial			
Port	27	Feature Key	0
DN	0550		
Start DN Discovery			
OK Default Send Retrieve Help			

Configuring the RLC system information

To configure the RLC system information:

- 1 Complete the fields as described in "RLC System Configuration field descriptions" on page 152.
- 2 Click on the **OK** button to save your settings to a temporary work file.
- 3 Click on the **Send** button to update the RLC with the new information.

Result: The RLC writes the changes to a temporary file on the administration PC.

Note: To save changes to the RLC's flash memory, select Upload → Save to Flash from the Menu Bar.

RLC System Configuration field descriptions

Field	Description
Unit ID	The RLC's Unit ID is 254 and cannot change. The remote units in a Remote Office system must have Unit IDs unique among those units connected to the same RLC. Note: This Unit ID must also be entered on the RLC Connection Configuration property sheet pertaining to each remote unit. With this information, the system creates the communication path between the remote unit and this RLC.
Node Name	Enter a descriptive name for this RLC.
Voice Activity Detection: Disable	Click on the Disable option button if you do not want the RLC to stop sending voice packets across the network when no one is speaking.
Voice Activity Detection: Enable	Click on the Enable option button if you want the RLC to stop sending voice packets across the network when no one is speaking.

Field	Description
Jitter Buffer	Select the length of time, in milliseconds (ms), that you want the RLC to collect unevenly arriving voice packets so that it can relay them evenly. This action works to lessen audible jitter.
Trunk Support	These option buttons allow you to configure the speed of your Remote Office connection. ■ Click on the 64K option button if the speed of your Remote Office connection is 64 Kbps. ■ Click on the 56K option button if the speed of your Remote Office connection is 56Kbps. ■ Click on the Dynamic option button if your Remote Office connection includes segments at 56Kbps and segments at 64Kbps.
DSP Gain	Select the number of decibels (dB) that you want to add to, or subtract from, the strength of the incoming signal before the DSP processes it. Valid options are: 9, 6, 3, 0, -3, -6, -9, -12, and -15. Note: Change this setting at the Host site to address a problem with signal strength at the remote site.
TALC ID	
Status: Disable	Refer to page 149 for information on the Integrated Digital Voice Recorder (IDVR).
Status: Enable	
IP Address	

Field	Description
Enable DN Discovery	■ Click in the Enable DN Discovery checkbox if you want the RLC to autodetect the PBX-configured name and number assigned to each line key for each remote port on the RLC. Note: For DN Discovery to work on any key other than key 0, you must enable TDD class of service on the host PBX. ■ Click on the Disable DN Discovery checkbox if you don't want the RLC to perform DN Discovery.
Frequency	Click on the option button that identifies how often DN discovery should be performed: ■ Once a Day ■ Once a Week ■ Once a month
Time	Specify the time when DN discovery should be performed.
Day	Select the day when DN discovery should be performed (if you selected "Once a Week" in the Frequency field).
Date	Specify the date when DN discovery should be performed (if you selected "Once a month" in the Frequency field).
RLC Extension to Dial	These fields allow you to configure one RLC port whose port number, feature key position, and DN are known. At the DN discovery time, each remote port on the RLC places a call to the DN in the RLC Extension to Dial field and the incoming CLID name and number is assigned to the calling port for use by the remote unit: ■ Port—This list box allows you to specify the remote site ■ Feature Key—This list box sets the feature key that initiates DN discovery ■ DN—This field displays the directory number to dial to access the remote unit

Field**Description****Start DN Discovery**

Click on the **Start DN Discovery** button to perform an unscheduled DN Discovery.

Understanding the IP interface

To operate as a node on the IP network, the following elements must be configured on the RLC:

- an IP address
- a subnet mask
- the default gateway

These items provide the network connection between the RLC, an administration terminal, and the remote site to allow the following to take place:

- Voice traffic is routed over the IP network between the RLC and the remote site.
- An administrator can use a PC located anywhere on the network to connect with any RLC or Meridian unit on the network.

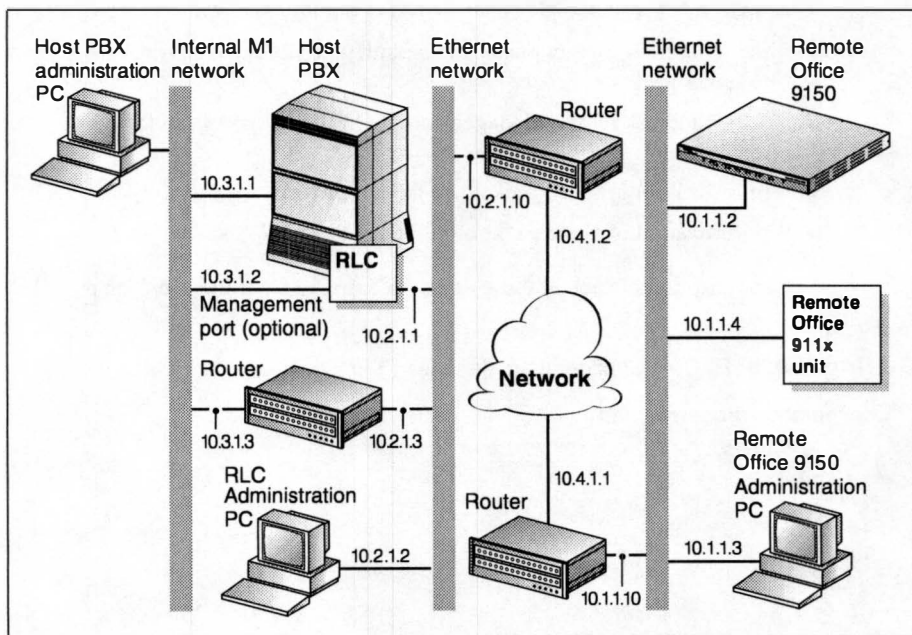
Once connected, you can view or work with the system configuration.

Note: To do this, the Configuration Manager software must be installed on that PC.

In addition to the IP address, subnet mask, and default gateway mentioned above, you can also assign an IP address to the management port on the RLC. Once you assign this IP address, you can use the PBX administration PC to log on to and administer the RLC through the host PBX's internal network.

Reach Line Card position in your IP network

As discussed earlier in this guide, the RLC is connected to a hub on your IP network. The following diagram provides an example of what the setup and the IP configuration look like:



G029

IP Configuration

Configure the RLC's IP connectivity on the IP Configuration property sheet. This section explains how to enter the following information:

- the IP address, subnet mask, and default gateway for the primary RLC Ethernet port
- the IP address for the Management RLC Ethernet port used for PBX maintenance over Ethernet
- prioritization of voice packets on the IP network
- prioritization of voice packets on the LANs and WANS

For a description of each of these items, refer to "IP Configuration" on page 158.

Getting there RLC → Configuration Manager → IP Configuration

IP Configuration property sheet

The screenshot shows the 'IP CONFIGURATION' dialog box. It has a title bar and a main area with several sections. The 'IP Information' section contains three rows of IP address input fields: 'IP Address' (1.0.0.0), 'IP Subnet Mask' (255.0.0.0), and 'IP Gateway' (0.0.0.0). The 'Management IP Information' section has a 'Disable' checkbox checked, and two rows of IP address input fields for 'Management IP Address' and 'Management IP Mask'. The 'QoS serv CodePoint' section has 'Enable' and 'Disable' radio buttons, with 'Disable' selected. The '802.1p Mapping' section also has 'Enable' and 'Disable' radio buttons, with 'Disable' selected. At the bottom, there are five buttons: 'OK', 'Default', 'Send', 'Retrieve', and 'Help'.

Configuring the IP addresses

To configure the IP addresses:

- 1 Enter the RLC's IP address in the IP Address fields.
Press the **Tab** key twice to move to the IP Network Mask row.
- 2 Enter the subnet mask in the IP Network Mask fields.
- 3 Enter the gateway's IP address in the IP Gateway fields.

IF you want to

THEN do the following steps.

establish the RLC on the host PBX's internal network

- 1 Click on the Management IP Information:Disable check box.

Result: The check mark in the check box disappears and Configuration Manager enables the Management IP Address and Management IP Mask fields.

- 2 Proceed to step 3.

not establish the RLC on the host PBX's internal network

- Proceed to step 5.

Note: The second Ethernet port of the RLC is only available with the RLC Multi-I/O cable—Enhanced.

- 3 Enter the IP address of the RLC's second Ethernet port in the Management IP Address fields.
- 4 Enter the subnet mask of the RLC's second Ethernet port in the Management IP Mask fields.
- 5 Click on the **OK** button.
- 6 Click on the **Send** button to update the RLC with the new information.

Result: Configuration Manager writes the changes to a temporary file on the administration PC.

Note: To save changes to the RLC's flash memory, select Upload → Save to Flash from the Menu Bar.

IP Configuration field descriptions

Field	Description
IP Address	Enter the IP address of the RLC.
IP Network Mask	Enter the IP network mask of the RLC.
IP Gateway	Enter the IP gateway of the RLC.
Management IP Information: Disable	■ Click in the Enable check box if you want to assign an IP address on the host PBX's internal LAN to the RLC. ■ Click in the Disable check box if you do not want to assign an IP address on the host PBX's internal LAN to the RLC. Since this is the default setting, you only need to do this after you have enabled management IP information. To assign the RLC an IP address on the host PBX's internal LAN, click in this check box. Result: The check mark disappears and Configuration Manager enables the Management IP Address and Management IP Mask fields.
Management IP Address	Enter the IP address of the RLC on the host PBX's internal LAN.
Management IP Mask	Enter the IP network mask of the host PBX if you do want remote units connected to this RLC to have the ability to configure PBX settings.
DiffServ CodePoint	■ Click on the Enable option button if you want to allow prioritization of voice packets sent from this RLC over WAN portions of the network. ■ Click on the Disable option button if you do not want to allow prioritization of voice packets sent from this RLC over WAN portions of the network.

Field	Description
802.1p mapping	■ Click on the Enable option button if you want to allow prioritization of voice packets sent from this RLC over LAN portions of the network. ■ Click on the Disable option button if you do not want to allow prioritization of voice packets sent from this RLC over LAN portions of the network.

Prioritizing voice traffic over shared networks

Prioritizing voice traffic on shared networks can improve QoS on LAN and WAN segments of the network that support prioritization. Achieving the desired QoS through prioritization over LAN connections requires you to enable 802.1p mapping. Achieving the desired QoS through prioritization over WAN connections requires you to enable the DiffServ Codepoint.

RLC port configuration

Ports on the RLC can be configured as one of the following ports:

- Remote ports provide host-PBX access to a remote user station. Configure at least one Remote port for each remote unit (Remote Office 9150, 9115, 9110 unit, or Meridian Digital Telephone IP Adapter) and for each Bridge port configured on a Remote Office 9150 unit.

Note: Bridge ports, configured on Remote Office 9150 units, allow the 9150 unit to give incoming, local, PSTN calls access to the following PBX features: Transfer, Call Forward, and Conference.

- Network ports establish PSTN connections between the RLC and its remote units.

Note: A common mistake in programming a PSTN connection is to enable only a single port (typically Port 16) on the RLC. Keep in mind, that one port must be programmed for each ISDN call that the Remote Office 9150 unit can place to the PBX. Note that typically a BRI line from a CO has the capability of placing two ISDN calls (2 B-channels) and therefore would require two network ports to be configured on the RLC. Refer to the PBX configuration notes for Class of Service requirements.

- Local ports provide local digital telephone connections directly to the RLC.

The following table describes port number ranges and how they can be configured.

Ports	Can be assigned to
0 through 15 and 32 through 47	digital telephone sets that are assigned to remote users. Note: The associated ports on the host PBX must be configured with voice capability.

Ports

16 through 31 and
48 through 63

Can be assigned to

- stations equipped with ATAs or MCAs

Note: For ATA and MCA compatibility with Remote Office 911x series units, refer to “Network port configuration” on page 110.

- network ports for configuring a trunk between the RLC and a remote unit.

Note: The associated ports on the host PBX must be configured with data capability.

Getting there RLC → Configuration Manager → RLC Port Configuration

RLC Port Configuration property sheet

Port	Remote	Network Port	Local TCM	Status	Configure
0	☐	☐	☐	Status: Dedicated, Priority: Normal, Compress	Configure
1	☐	☐	☐	Status: Dedicated, Priority: Normal, Compress	Configure
2	☐	☐	☐	Status: Dedicated, Priority: Normal, Compress	Configure
3	☐	☐	☐	Status: Dedicated, Priority: Normal, Compress	Configure
4	☐	☐	☐	Status: Dedicated, Priority: Normal, Compress	Configure
5	☐	☐	☐	Status: Dedicated, Priority: Normal, Compress	Configure
6	☐	☐	☐	Status: Dedicated, Priority: Normal, Compress	Configure
7	☐	☐	☐	Status: Dedicated, Priority: Normal, Compress	Configure
8	☐	☐	☐	Status: Dedicated, Priority: Normal, Compress	Configure
9	☐	☐	☐	Status: Dedicated, Priority: Normal, Compress	Configure
10	☐	☐	☐	Status: Dedicated, Priority: Normal, Compress	Configure
11	☐	☐	☐	Status: Dedicated, Priority: Normal, Compress	Configure
12	☐	☐	☐	Status: Dedicated, Priority: Normal, Compress	Configure
13	☐	☐	☐	Status: Dedicated, Priority: Normal, Compress	Configure
14	☐	☐	☐	Status: Dedicated, Priority: Normal, Compress	Configure
15	☐	☐	☐	Status: Dedicated, Priority: Normal, Compress	Configure

OK Default Send Retrieve Help

Configuring an RLC port

To configure an RLC port:

- 1 Click on the appropriate tab for the port you are configuring, as in Ports 0-15 or Ports 16-31 for a 16-port RLC, Ports 0-15, Ports 16-31, Ports 32-47, or Ports 48-63 for a 32-port RLC.
- 2 In the line for the port you are configuring, choose the type of port you want to configure as follows:

IF you want to configure a

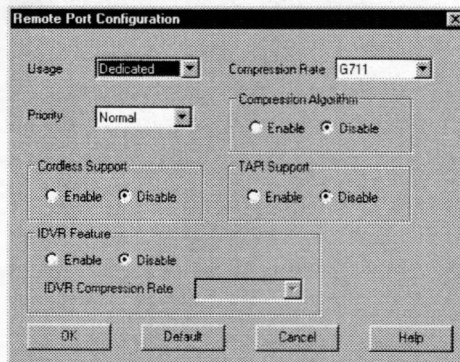
THEN

remote port,

complete the following steps:

- a Click on the **Remote** option button on the line of the port number you are configuring.
- b Click on the **Configure** button on the same line.

Result: The Remote Port Configuration dialog box displays, similar to the following:



- c Select the desired settings according to the “Remote port configuration field descriptions table” on page 166.
- d Click on the **OK** button to save the information to a temporary file on your administration PC.

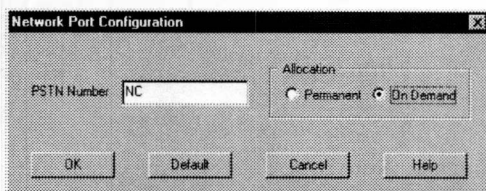
**IF you want to
configure a****THEN**

network port,

complete the following steps:

- a Click on the **Network Port** option button on the line of the port number you are configuring.
- b Click on the **Configure** button on the same line.

Result: The Network Port Configuration dialog box displays, similar to the following:



- c Select the desired settings according to the “Network port field descriptions table”, on page 169.
- d Click on the **OK** button to save the information to a temporary file on your administration PC.

- 5 Click on the **Send** button to update the RLC with the new information.

Result: The administration PC saves the changes in a temporary file.

- 6 To save changes to the RLC's flash memory, select Upload → Save to Flash from the Menu Bar.

Note: Refer to page 149 for information on the Integrated Digital Voice Recorder (IDVR).

Remote port configuration field descriptions table

Field	Description
Usage	■ Select Dedicated if this you use this port for one DN only. ■ Select Multiuser if a variety of remote units or different ports on the same remote unit can use this port in a time-share fashion. ■ Select Dynamic Pool if this port is part of a dynamic pool and can be assigned to any remote port requesting access to any port of the RLC pool.
Compression Rate	Select the compression that offers the voice quality and network bandwidth you want for calls on this port. Valid options are: G.711, G.726, G.729, and G.729/FAX.
Priority	■ Select PSTN only to allow access only to the PSTN. PSTN-only ports do not move between networks according to QoS levels. Meridian telephones that place calls to PSTN only telephone sets when there is not enough PSTN bandwidth available receive an error message. In this situation, Bandwidth Limit appears on the calling telephone's display. ■ Select High to allow access either to the PSTN or the IP network, based on QoS. Calls through High priority ports move to the PSTN first in a QoS transition. In recovery situations, when IP QoS returns to within configured limits, calls through High priority ports return to the IP network last, ensuring the most consistent QoS.

Remote port configuration field descriptions table (Continued)

Field	Description
Priority (Continued)	■ Select Normal to allow access to either the PSTN or the IP network, based on QoS. Calls through Normal priority ports move to the PSTN only after all calls through High priority ports make the transition. In recovery situations, as QoS on the IP network returns to within configured limits, calls through Normal priority ports return to the IP network first. ■ Select IP only to allow access only to the IP network. IP-only ports do not move between networks according to QoS levels.
Compression algorithm	■ Click on the Enable option button if you want to allow compression on this port. ■ Click on the Disable option button if you do not want to allow compression on this port.
Cordless Support	RLC ports can support either corded telephones or cordless telephones. ■ Click on the Enable option button if you want this port to provide service only to cordless telephones, such as M2616CT. ■ Click on the Disable option button if you want this port to provide service only to corded telephones, such as M2616. Note: Misconfiguration of this field causes incorrect remote telephone operation.

Remote port configuration field descriptions table (Continued)

Field	Description
TAPI Support	Enabling Telephone Application Programming Interface (TAPI) support allows telephones using the selected port to interact with a TAPI server such as Meridian Communicator. ■ Click on the Enable option button if you want this port to interact with a TAPI server. ■ Click on the Disable option button if you want to prevent this port from interacting with a TAPI server. When configured for TAPI support, the RLC allocates DSP and bandwidth resources whenever a line key indicator goes active and stays active for Multiple Appearance DNs. To prevent the over-allocation of these resources during midnight routines, either disable LD 35, or configure the RLC as Offline during this period. Note: You must configure MSL-100 ATA sets and MSL-100 AAB sets for TAPI support for them to function properly.
IDVR Feature	Refer to page 149 for information on the Integrated Digital Voice Recorder (IDVR).
IDVR Compression Rate	

Network port field descriptions table

Field	Description
PSTN Number	Enter the DN of the port you are configuring in the PSTN Number field.
Allocation	The allocation setting refers to the connection status of the port you make the setting for. ■ Click on the Permanent option button if you want connections established over the port you are configuring to remain up until the remote unit goes offline. ■ Click on the On Demand option button if you want connections established over this port to go down when they are no longer needed. Connections over ports configured as On Demand remain up until the minimum call duration timer expires.

IDVR Feature Key Configuration field descriptions table

Field	Description
IDVR Status	
Key Feature	Refer to page 149 for information on the Integrated Digital Voice Recorder (IDVR).
Key Number	
IDVR Compression Rate	

Remote Connection Configuration

This section shows you how to choose the following settings for each remote unit:

- security
- IP connection
- PSTN connection
- call timers

Getting there RLC → Configuration Manager → Remote Connection Configuration

Remote Connection Configuration property sheet

The screenshot shows a 'REMOTE CONNECTION CONFIGURATION' dialog box. It contains several sections for configuring a remote unit. At the top, there are fields for 'Unit ID' (a dropdown menu) and 'Unit Type' (a text field with '9150' entered). To the right is a 'Status' section with 'Enable' and 'Disable' radio buttons. Below this is a 'Security' section with a 'Security Level' dropdown (set to 'No security') and 'Inbound' and 'Outbound' text fields. The 'IP' section has 'Status' radio buttons (Enable/Disable), a 'Configure' button, and 'IP Address' fields. It also has an 'IP Bandwidth' field. The 'PSTN' section has 'Status' radio buttons, a 'Configure' button, a 'PSTN Number' field, and 'Bandwidth' fields for 'Extra' and 'Priority Reserved'. There are also 'Dedicated PSTN n/w Port' and 'Callback for PSTN' fields. At the bottom, there are 'User On Demand Idle Timer' and 'User On Demand Min Call Times' fields, both set to '30'. There is also an 'IDVR Feature' section with 'Enable' and 'Disable' radio buttons. At the very bottom are buttons for 'Online/Offline', 'Quality of Service', and 'Caller ID'. The dialog box has 'OK', 'Default', 'Send', 'Retrieve', and 'Help' buttons at the bottom.

Security

The RLC offers three security levels. For an explanation of each of these levels, refer to “Multiple security levels” on page 17.

To configure security for the RLC:

- 1 Choose the desired security level in the Security Level drop down box on the Remote Connection Configuration property sheet.
- 2 If you select Provisioned security, you must also enter a 10-digit Outbound Security identifier and a 10-digit Inbound Security identifier. To see how these Security identifiers effect RLC and Remote Office operation, refer to “Multiple security levels” on page 17.

IP connection

To allow a remote unit to establish VoIP connection with the RLC:

- 1 Enable the VoIP functionality on the IP network for that unit by selecting the option button located in the Status section.
- 2 Select the Yes option button located in the IP: Configure section.
- 3 Enter the unit's IP address in the IP Address fields.
- 4 Determine the IP Bandwidth using data rate values provided in the Bandwidth usage table located in the *Remote Office Network Engineering Guidelines* (NTP 555-8421-103). Calculate the number of simultaneous calls allowable on your WAN. This depends on the following information:
 - compression algorithms used by the call (refer to the table below)
 - your Wide Area Network (WAN) type
 - whether Voice Activity Detection (VAD) is enabled or disabled

Compression algorithm	Required voice bandwidth in Kbps
G.711	64
G.726	32
G.729	8
G.729/FAX	14.4

IP Bandwidth calculation examples (using Peak Data Rate values):

- For a one Mbyte Frame Relay WAN supporting only G.711 calls, enter 848 in the IP Bandwidth field according to the following calculation:
 $1024\text{K} (1 \text{ Mbyte}) - 16\text{K for signaling} = 1008\text{K of available bandwidth}$
 $1008\text{K}/76\text{Kbps (peak data rate for a G.711 call according to the Bandwidth Usage table)} = 13$
therefore,
 $\text{IP Bandwidth} = (13 \text{ G.711 calls} * 64\text{K [required voice bandwidth from the table above]}) + 16\text{K (for signaling)} = 832 + 16 = \mathbf{848\text{K}}$
- For a one Mbyte Frame Relay WAN supporting only G.729 calls, enter 0 in the IP Bandwidth field according to the following calculation:
 $1024 (1 \text{ Mbyte}) - 16\text{K for signaling} = 1008\text{K of available bandwidth}$
 $1008/20\text{Kbps (peak data rate for a G.729 call according to the Bandwidth Usage table)} = 50$
therefore,
 $\text{IP Bandwidth} = (50 \text{ G.729 calls} * 8\text{K [required voice bandwidth according to the table above]}) + 16\text{K (for signaling)} = 400 + 16 = \mathbf{416\text{K}}$

Note: Since the maximum number of simultaneous calls possible through a Remote Office system is 32 calls, 50 simultaneous calls are not possible. Therefore, the proper IP Bandwidth setting is 0. Zero (0) is the setting for no bandwidth limit.
- For a 128K Frame Relay WAN supporting up to two G.726 and one G.729 call, enter 88 in the IP Bandwidth field according to the following calculation:
 $(2 \text{ calls} * 44\text{K [peak data rate for a G.726 call according to the Bandwidth Usage table]}) + (1 \text{ call} * 22\text{K [peak data rate for a G.729 call according to the Bandwidth Usage table]}) + 16\text{K (for signaling)} = 88 + 22 + 16 = 126\text{K}$
therefore,
 $\text{IP Bandwidth} = (2 \text{ G.726 calls} * 32\text{K required voice bandwidth from the table above}) + (1 \text{ G.729 call} * 8\text{K required voice bandwidth from the table above}) + 16\text{K (for signaling)} = (2 * 32) + (1 * 8) + 16 = 64 + 8 + 16 = \mathbf{88\text{K}}$

PSTN configuration

To allow a remote unit to establish PSTN connections with the RLC:

- 1 Enable PSTN functionality on the PSTN for the unit indicated in the Unit ID field by selecting the Enable option button located in the PSTN: Status section.
- 2 Select the Yes option button located in the PSTN: Configure section.
- 3 Enter the remote unit's DN in the PSTN Number field.

You must configure PSTN numbers including, the ISDN numbers, in a specific manner. Please read the following examples carefully.

Configuring seven-digit ISDN numbers

If the service documents supplied by the BRI service provider contain a seven-digit ISDN number, then choose from among the following options to configure the number on your Remote Office unit:

- Remote Office 9150 unit BRI configuration
Configure the PSTN numbers with the seven digits provided by the Central Office without area codes. For example:
 - 5551000 configured against the corresponding B-channel, not 2145551000
- RLC Remote Connection Configuration
Use the # delimiter to separate the Trunk Access code and area code part of the PSTN number. For example:
 - #9#5551000 (not 95551000) where "5551000" is the primary Remote Office 9150 B-channel
 - #91214#5551000 (if long distance between units), not 92145552000
- RLC Network Port configuration
Enter the Network Port PSTN Number exactly as the Remote Office unit must dial it. For example:
 - 5552000 (for seven-digit local call) where 5552000 is a PBX DID data port number
 - 12125552000 (if long distance)
 - 912125552000 (if long distance and the 9150 BRI CO uses a "9" access code)

Configuring 10-digit ISDN numbers

If the service documents supplied by the BRI service provider contains a 10-digit ISDN number, then the configuration is as follows:

- Remote Office 9150 BRI configuration
Configure the PSTN numbers with the 10 digits provided. For example: 2145551000 configured on the corresponding B-channel.
- RLC Remote Connection Configuration
Use the # delimiter to separate the Trunk Access code from the PSTN number. For example:
 - #9#2145551000 (not 92145551000) where “5551000” is the primary Remote Office 9150 unit B-channel and “9” is the Trunk Access Code.
 - #91#2145551000 (if long distance)
- RLC Network Port configuration
Enter the Network Port PSTN Number exactly as the Remote Office unit must dial it. For example:
 - 5552000 (for seven digit local call) where 5552000 is a PBX DID data port number
 - 12125552000 (if long distance)
 - 912125552000 (if long distance and the Remote Office 9150 BRI CO uses a 9 access code)

Configuring 911x PSTN connections

To configure a PSTN Remote Office 911x series unit:

- 1 Access the RLC Connection Configuration sheet in Configuration Manager.
- 2 Enter the DID number of the dedicated PSTN network port on the RLC for the Remote Office 911x series unit in the PSTN Number to Connect to RLC field.
- 3 Click on the **OK** button.

Special Configuration for Callback for PSTN

The Callback for the PSTN field on the RLC Remote Connection Configuration property sheet allows you to enable and disable Callback. The default is Callback for PSTN disabled. This means that the RLC places data calls to the Remote Office 9150 unit to establish additional bandwidth during normal operation. If you enable Callback for PSTN, the Remote Office 9150 unit places the call to the RLC to establish additional bandwidth.

Note: During a RLC or Remote Office 9150 reset, or during a sudden IP network failure, both the RLC and the Remote Office 9150 unit attempt to call each other to establish the Primary Signaling Link. When this occurs, either system can actually establish the first connection. Follow the guidelines below when configuring callback for PSTN.

If Callback for PSTN is disabled:

1. Configure the Primary Network Port with a DID number on the host PBX that is routed over a data capable PRI.
2. Configure either DID numbers or internal DNs on all other network ports (one per B Channel).

If Callback for PSTN is enabled:

1. Configure the Primary Network Port with a DID number on the host PBX routed over a data capable PRI.
2. Configure DID numbers on all other network ports (one per B Channel).

Minimum call duration timers and Idle timers

The RLC uses minimum call duration timers and idle timers to help control PSTN costs. For a detailed discussion of these timers, refer to “Timers” on page 20. For information on configuring these timers, refer to “User On Demand Idle Timer” and “User On Demand Min Call Timer” on page 181.

Configuring remote connection settings

To configure remote connection settings:

- 1 Complete the fields as described in "Remote Connection Configuration field descriptions" on page 178.
- 2 Click on the **OK** button to save the information in the temporary work file.
- 3 Click on the **Send** button to update the RLC with the new information.

Result: The RLC writes the changes to a temporary file on the administration PC.

Note: To save changes to the RLC's flash memory, select Upload → Save to Flash.

Remote Connection Configuration field descriptions

Field	Description
Unit ID	Select the site number assigned to the remote unit you are configuring. Valid options are: 1–20.
Unit Type	Select 911 X, or 9150 according to the Remote Office unit you are configuring at the remote site. Note: Only four Remote Office 9150 units can be connected to the same RLC.
Status	■ Click on the Enable option button to activate the remote unit. ■ Click on the Disable option button to deactivate the remote unit.
Security Level	Select the desired security level. Valid options are: No security, Caller ID security, or Provisioned security.
Security ID: Inbound	If you selected provisioned security, enter the Security ID, up to 10 digits in length, that must be presented by calls before they are received at this site.
Security ID: Outbound	If you selected provisioned security, enter the Security ID, up to 10 digits in length, that must be presented by calls before they are allowed to go out from this site.
IP: Status	Select whether or not VoIP is the primary connection type to the remote office. ■ Click on the Enable option button to choose the IP network as the primary connection type to the remote unit. ■ Click on the Disable option button to disable connectivity to the remote unit over the IP network.

Remote Connection Configuration field descriptions (Continued)

Field	Description
IP: Configure	Enable IP configuration to allow the RLC to initiate IP connections to the remote site. Note: You must also configure an IP address for the remote unit. ■ Click on the Enable option button to configure a static IP address for the remote unit. The RLC uses this address for connections to the remote unit. ■ Click on the Disable option button if you do not wish to configure an IP address for the remote unit.
IP Address	Enter the remote unit's IP address if you want to be able to initiate IP connections to the remote site from the RLC.
IP Bandwidth	Enter the total amount of voice bandwidth needed for the maximum number of simultaneously active telephone calls over your WAN.
PSTN: Status	To use the PSTN mode with this remote unit, you must enable PSTN connectivity. ■ Click on the Enable option button to allow the RLC to connect to the remote unit over the PSTN. ■ Click on the Disable option button to prevent the RLC from connecting to the remote unit over the PSTN.
PSTN: Configure	To allow the RLC to initiate a PSTN connection to the remote site, you must configure a PSTN number for the remote unit. ■ Click on the Yes option button to configure the remote unit's PSTN number. ■ Click on the No option button if you do not wish to configure the PSTN number for the remote unit.

Remote Connection Configuration field descriptions (Continued)

Field	Description
PSTN Number	Enter the PSTN number the RLC must dial to connect to the remote unit. For configuration details, refer to “PSTN configuration” on page 174.
Dedicated PSTN n/w (network) Port	Enter the RLC network port number that is dedicated to support the remote unit. Note: All network ports that are not dedicated are used as a pool to support additional network connections to remote units.
Bandwidth: Extra	Enter the minimum number of Kbytes of bandwidth to have available at any time for PSTN access to the remote unit.
Bandwidth: Priority Reserved	Enter the Kbytes of PSTN bandwidth you would like to reserve for high priority DNs.
Callback for PSTN	The Callback for PSTN setting determines the site that initiates additional trunk connections when the RLC identifies the need for additional bandwidth. ■ Click on the Enable option button if you want the Remote Office 9150 unit to initiate the additional trunk connections. ■ Click on the Disable option button if you want the RLC to initiate the additional connections.
User On Demand Idle Timer	Enter the maximum number of seconds that a PSTN connection can remain idle at this remote site before the RLC closes it. For more details, refer to “Minimum call duration timers and Idle timers” on page 176.

Remote Connection Configuration field descriptions (Continued)

Field	Description
User On Demand Min Call Timer	Enter the minimum number of seconds that a PSTN connection must remain open at this remote site before the RLC closes it. For more details, refer to “Minimum call duration timers and Idle timers” on page 176.
IDVR Feature	Refer to page 149 for information on the Integrated Digital Voice Recorder (IDVR).
Online/Offline	Click on the Online/Offline button to edit the online/offline table for this remote site. Refer to “Online/Offline table configuration” on page 189 for details on configuring this table.
Quality of Service	Click on the Quality of Service button to edit the QoS Transitioning Technology settings for this remote site. Refer to “Configuring Quality of Service” on page 182 for information on configuring these settings.
Caller ID	If you have chosen caller ID security for this remote site, click on the Caller ID button to enter the telephone numbers that you want to have access to this remote site.

Configuring Quality of Service

This section shows you how to configure the RLC with quality and duration values for Nortel Networks' patented QoS Transition Technology.

QoS Transitioning Technology allows you to define *acceptable* voice QoS for Remote Office telephone calls routed using Voice over Internet Protocol (VoIP). The Signal Degrade slide control allows you to set the point where poor voice QoS causes the RLC to transition calls to the PSTN for better QoS. The Signal Recover slide control identifies the IP voice QoS level where you want the RLC to recover calls to the IP network.

You can also define the following duration parameters:

- The degrade duration is the time (in seconds) that QoS must remain below the degrade threshold before the RLC transitions calls to the PSTN.
- The recover duration is the time (in minutes) that QoS must remain above the recover threshold before the RLC recovers the call to the IP network.

The units of the acceptable duration for recovery are minutes rather than seconds in an attempt to minimize *transition thrashing*. Transition thrashing is the rapid transition and recovery between networks. This can occur when QoS hovers around configured degrade and recover thresholds. This phenomenon produces higher than normal PSTN charges.

Note: Quality of Service problems can sometimes be addressed through prioritization of voice packets. For more information, refer to "Quality of service on shared networks" on page 15.

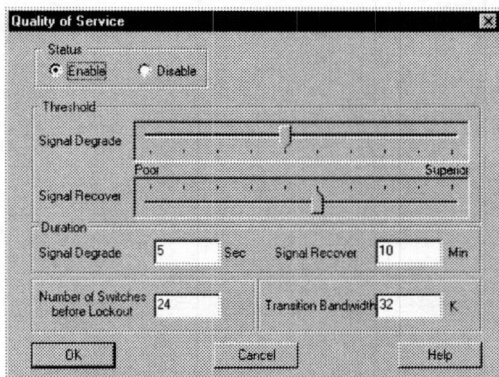
More information

Refer to the *Remote Office Network Engineering Guidelines* (NTP 555-8421-103) for detailed information describing QoS Transitioning Technology. To locate this document, click on the Customer Support, Documentation, and North America links at the following website:

www.nortelnetworks.com

Getting there RLC → Configuration Manager → Remote Connection Configuration
→ Quality of Service

Quality of Service dialog box



Configuring QoS

The slide controls allow 10 settings ranging from poor to superior, within the following boundaries:

- 1 (poor) equates to a MOS—mean opinion score—value of 3.0, as calculated by the RLC and based upon the ITU E-Model for serviceability and service integrity performance
- 10 (superior) equates to a MOS value of 4.0

Since the ITU E-Model uses network delay as its sole point of reference, the RLC also factors in average packet-loss to obtain the MOS value. For example, if the user sets the threshold to a MOS value of 3.5 (center tick of slide control), the following scenario can occur. The measured delay on the network may indeed be less than a score of 3.5 according to the ITU E-model. However, excessive packet loss can lower the MOS value calculated by the RLC. In this scenario, the RLC moves the call from the IP network to the PSTN. This move ensures an acceptable quality of service for the user, based on real network conditions.

QoS configuration procedure

- 1 Complete the fields as described in "Quality of Service field descriptions table" on page 185.
- 2 Click on the **OK** button to save the information in the temporary work file.
- 3 Click on the **Send** button to update the RLC with the new information.

Result: The RLC writes the changes to a temporary file on the administration PC.

- 4 To save changes to the RLC's Flash memory, in the Menu Bar select Upload → Save to Flash.

Quality of Service field descriptions table

Field	Description
Status	■ Click on the Enable option button to allow QoS transitions to occur when the QoS on the IP network degrades. ■ Click on the Disable option button if you do not want to use the QoS Transitioning Technology.
Threshold: Signal Degrade	Move the indicator to the appropriate point on the sliding scale, a relative value between poor and superior.
Threshold: Signal Recover	Move the indicator to the appropriate point on the sliding scale, a relative value between poor and superior.
Duration: Signal Degrade	Enter a value, in seconds, between 1 and 60. If poor voice quality lasts for the specified duration, then calls are moved from the IP network to the PSTN.
Duration: Signal Recover	Enter a value, in minutes, between 1 and 10. When the improved voice quality lasts for the duration value chosen (in minutes), then calls are moved back to the IP network.
Number of Switches before Lockout	Enter the number of transitions between the IP network and PSTN in any 24-hour period that causes the RLC to stop making the transition.
Transition Bandwidth	Enter the amount of bandwidth in Kbytes that you want the RLC to have available at all times for use when transitioning between the IP network and PSTN.

How the online/offline table works

Use the online/offline table to schedule the times that the RLC makes a PSTN connection available to an RLC port. The online/offline table gives you the ability to ensure that potentially costly PSTN/ISDN or long distance connections do not stay up after business hours. If the offline command occurs while the connection is in use, Remote Office system users at the remote site can override table settings.

Notes:

- When a remote unit is in the offline mode, users cannot place host-controlled calls with that unit.
- Users can override the online/offline table to establish or terminate a connection to the network.

Online/offline configuration example

The online/offline table allows you to make up to eight entries per day, every day of the week, for each remote site. The following is an example of a standard online/offline program for an RLC port.

Entry	State	State
Entry 1	At 8:00 a.m., the RLC establishes the remote site's PSTN connection.	Online
Entry 2	At 11:30 a.m., (a common lunchtime) the RLC disables the PSTN connection.	Offline
Entry 3	At 12:30 p.m., (the end of lunchtime) the RLC re-enables the PSTN connection.	Online
Entry 4	And at 5:00 p.m., the RLC disables the PSTN connection for the day.	Offline

Online/Offline table overrides

Any remote user can override the settings of the online/offline table if the table attempts to terminate the connection during a call. A buzz alerts users at the remote site that the connection is going down in 30 seconds. After the initial warning, users can enter the online SPRE code on their telephone key pads to override the termination of the connection. The warning buzz repeats itself 20 and 10 seconds before the system terminates the connection. Any user at the remote site can avoid going offline by entering the online SPRE code.

Multiple offline periods

You can configure multiple offline entries into the table without configuring online entries between each offline entries. In this way, you can program the RLC to terminate a connection that has been left open should a remote site user be forced to override a scheduled PSTN termination.

For example, Mr. Smith, a remote site user, begins a business call with Mr. Jones, at 4:45 p.m. on a Friday. The RLC is programmed to terminate his PSTN connection at 5:00 p.m. However, Mr. Smith overrides the scheduled termination, and the call continues for another 45 minutes. The business call succeeds, but the expensive PSTN connection remains up. If the usual schedule were followed, the connection would not be terminated until lunch time on the following Monday.

Fortunately, Mr. Smith's system administrator foresaw this situation and configured offline commands for 6:00, 7:00, and 8:00 p.m. So, the RLC terminates the PSTN connection at 6:00 p.m. Mr. Smith's company accrues only 15 minutes of unnecessary PSTN charges.

How the remote site goes online

When going offline, the remote unit's offline timer activates. When the timer expires, the remote unit automatically initiates a "going online" request to the host PBX. If the RLC receives the request successfully, the remote site and its associated digital telephones go online.

If you configure no online entries in the online/offline table, the RLC instructs the remote unit to go offline forever each time it processes an offline entry. To go back online, a remote user must enter the online SPRE code in order to place host-controlled calls on either the PSTN or IP network.

Online/Offline table configuration

The Online/Offline Table allows you to enter up to eight entries per day for each remote site, every day of the week. You can define each entry as Online, Offline, or Undefined.

Getting there RLC → Configuration Manager → Remote Connection Configuration
→ Online/Offline Table

Online/Offline Table

State	Time
Undefined	00:00
Undefined	00:00
Undefined	00:00
Undefined	00:00
Undefined	00:00
Undefined	00:00
Undefined	00:00
Undefined	00:00

Configuring an Online/Offline Table

To configure the Online/Offline Table:

- 1 Access the Remote Connection Configuration property sheet.
- 2 Ensure that the Unit ID drop down box shows the Unit ID for the remote unit you want to configure an Online/Offline Table for. If it does not, choose the proper Unit ID from the drop down box, such as **1—20**.
- 3 Ensure that the Unit Type drop down box properly reflects the remote unit you want to configure an Online/Offline Table for. If it does not, choose the proper Unit Type from the drop down box, such as **9150** or **911X**.
- 4 Click on the **Online/Offline** button.

Result: The Online/Offline Table dialog box displays. (Refer to "Online/Offline Table" on page 189.)

- 5 From the Day drop down box, select the day of the week that you want the remote unit to have access to the network (PSTN or IP).
- 6 In the enabled State drop down box, choose **Online** or **Offline**, according to the command you want the system to initiate for this remote site.

Result: Configuration Manager enables the associated Time list box and the State and Time list boxes immediately below. The chosen state (**Online** or **Offline**) displays in the list box described in step 6.

Note: If you choose **Undefined**, the subsequent list boxes remain disabled. Configuration Manager takes your choice of **Undefined** to be an indication that you do not want to configure more commands in this Online/Offline Table.

- 7 In the associated Time list box, choose the time (24-hour time format) that you would like Configuration Manager to initiate the state chosen in step 5.
- 8 As you make selections in the State drop down box, Configuration Manager enables list boxes in the subsequent line, with the opposite selection.

chosen as a default selection. For example, **Offline** (if you chose **Online** in step 6) or **Online** (if you chose **Offline** in step 6).

Note: You can make your desired Online/Offline Table selection in any enabled box in any order.

IF you want to**THEN**

continue configuring entries (up to eight) in the Online/Offline Table for this remote unit,

return to step 6.

stop configuring the Online/Offline Table for this remote unit,

click on the **OK** button.

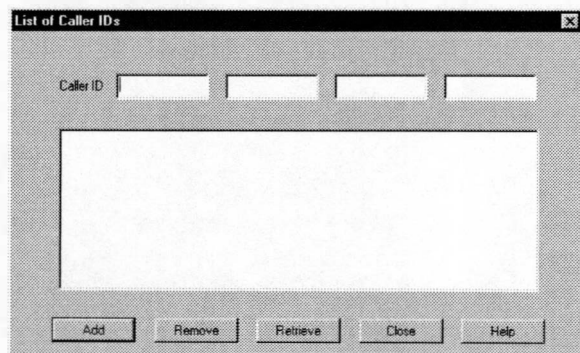
Caller ID configuration

Note: This procedure applies to Remote Office 9150 units only.

In the list of Caller IDs dialog box, enter the DNs of every B-channel assigned to the remote unit you are configuring. The Unit ID field of the associated Remote Connection Configuration property sheet identifies the remote site these Caller IDs apply to. Enter up to 20 telephone numbers using the same format used by the PSTN for presenting these DNs, such as 10 digits or four digits. If you want to use level 2 (Caller ID) security, you must enter the DNs of all associated B-channels. For more information on Caller ID security, refer to “Level 2, caller ID security” on page 17. For the proper procedure to use in Caller ID configuration, refer to “Configuring Caller ID information” on page 193.

Getting there RLC → Configuration Manager → Remote Connection Configuration
→ Caller ID

List of Caller IDs



Configuring Caller ID information

To configure Caller ID information for a Remote Office 9150 unit:

- 1 Access the Remote Connection Configuration property sheet. (Refer to "Remote Connection Configuration" on page 171 for help in locating this property sheet.)

- 2 Choose the Unit ID of the Remote Office 9150 unit that you want to configure Caller IDs in the Unit ID drop down box, such as **1–20**.

Result: 9150 appears in the Unit Type drop down box. If 9150 does not appear in the Unit Type drop down box, for instance, if you are completing an offline configuration, select 9150 from the available options.

- 3 Click on the **Caller ID** button.

Result: The Caller ID configuration sheet appears. (Refer to "List of Caller IDs" on page 192.)

- 4 Enter the telephone numbers of the people to whom you want to grant access to the remote unit in the Caller ID fields.

Note: Enter up to four Caller IDs.

- 5 Click on the **Add** button.

Result: The numbers you entered in the fields appear in the larger window below.

- 6 When you have entered all of the Caller IDs for the ISDN BRI B-channels assigned to this Remote Office 9150 unit, you can configure up to 8, click on the **Close** button.

Result: The List of Caller IDs dialog box disappears and Configuration Manager returns you to the Remote Connection Configuration property sheet.

- 7 Click on the **OK** button to save the information in the temporary work file.

- 8 Click on the **Send** button to update the RLC with the new information.

Result: The RLC writes the changes to a temporary file on the administration PC.

Note: To save changes to the RLC's flash memory, select Upload → Save to Flash.

DSP configuration

This section shows you how to configure DSP resources on your RLC. The RLC must provide the same number of voice DSP channels as the maximum number of simultaneous calls your remote services network supports. Each DSP *module* holds two DSP *devices*. Currently, each DSP *device* holds four DSP *channels*. To add eight DSP *channels* to your Remote Office system's voice processing capability, add one DSP application *module*.

Calls made from Remote Office 911x series units require two DSP channels (one voice channel, one modem channel) when operating in PSTN mode. This includes QoS transitions. If you want to configure Remote Office 911x series units for analog modem calls, you must set the RLC DSPs to Remote Office 911x. Each DSP configured for the Remote Office 911x series unit supports four modem only connections (no support for G.711, G.729, or G.726).

Getting there RLC → Configuration Manager → DSP Configuration

DSP Configuration property sheet

DSP CONFIGURATION

Module Number

0

▼

No of Devices:

Device Number 1

DSP Load

AUTO

▼

Compression Algorithms

G729

G726

G711

Device Number 2

DSP Load

AUTO

▼

Compression Algorithms

G729

G726

G711

OK

Default

Send

Retrieve

Help

194

RLC Installation and Administration Guide

Module identification

The upper portion of the DSP configuration property sheet displays fields that identify the module you are currently configuring. In the Module Number drop down box, choose the module position on the RLC that the DSP module occupies. Module 0 represents the built-in DSP resources on the RLC—the equivalent of one DSP application module.

Device configuration

The middle portion of the property sheet displays information describing the DSP loads, and corresponding compression algorithms that you can select for each DSP device.

Configuring DSPs

To configure DSP modules on your RLC, complete the following steps:

- 1 Access the DSP Configuration property sheet.
- 2 Complete the fields as described in "DSP Configuration field descriptions" on page 196.
- 3 Click on the **OK** button to save the information in the temporary work file.
- 4 Click on the **Send** button to update the RLC with the new information.

Result: The RLC writes changes to a temporary file on the administration PC.

Note: To save changes to the RLC's flash memory, select Upload → Save to Flash.

DSP Configuration field descriptions

Field	Description
Module Number	Select the number of the module DSP position on the RLC occupied by the DSP application module you are configuring. Valid options are: 1–4.
No of Devices	This is a read-only field displaying the number of DSP devices on the application module in the selected module position. Refer to “DSP configuration” on page 194 for an explanation of DSP <i>devices</i> versus DSP <i>modules</i> and DSP <i>channels</i> .
DSP Load Note: This description applies to both appearances of this field.	Select the DSP load that you want to enable on this DSP device. Valid options are: G729, 911X, AUTO. Note: Selecting AUTO instructs the RLC to choose a <i>default</i> DSP load. This <i>default</i> load is G.729, depending on DSP channel availability.
Compression Algorithms Note: This description applies to both appearances of this field.	This read-only field displays the compression algorithms contained in DSP load displayed in the DSP load drop down box. The compression algorithm (G.711, G.726, or G.729) used on calls to or from the Remote Office unit stations is dictated by the compression setting configured for the remote port over which the call is processed.

Chapter 7

Administration

In this chapter

Changing the administration password	198
Creating a backup configuration file	200
Restoring the configuration	203
Display logs	208
Statistics screens	212
Verifying the firmware and software version	245
Obtaining the latest upgrade file	247
Performing a firmware upgrade	248
Performing a software upgrade	252

Changing the administration password

Two layers of password security protect the RLC's configuration. If you want to secure the RLC's configuration so that only those with passwords unique to your RLC can make configuration changes, alter the following items:

- Configuration Manager password
This password prevents unauthorized users from performing offline configuration changes.
- RLC's password
This password prevents unauthorized users from performing online changes of the configuration residing in the RLC's Flash memory.

Note: Make sure that you record the password and store it in a safe, secure location. If you forget or lose the password, contact your Nortel Networks customer support representative.

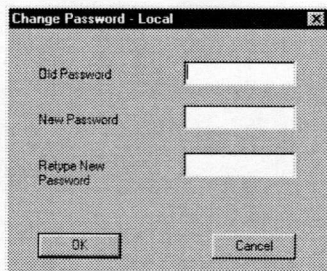
Getting there RLC → Configuration Manager

Changing the Configuration Manager password

To change the Configuration Manager (local) password:

- 1 From the Menu Bar, choose Connect → Change Password → Local.

Result: The Change Password dialog box displays, similar to the following:

A screenshot of a Windows-style dialog box titled "Change Password - Local". It contains three text input fields labeled "Old Password", "New Password", and "Retype New Password". At the bottom of the dialog are two buttons: "OK" and "Cancel".

- 2 Complete the fields in the Change Password dialog box.

- 3 Click on the **OK** button.

Result: The Password changed successfully dialog box displays.

- 4 Click on the **OK** button.

Changing the RLC password

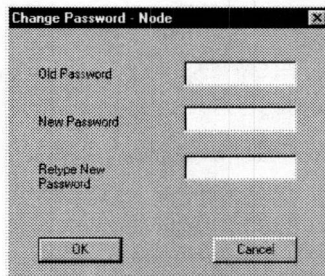
To change the RLC (node) password:

ATTENTION

Do not change the RLC's password until the system is up and working.

- 1 From the Menu Bar, choose Connect → Change Password → Node.

Result: The Change Password dialog box displays, similar to the following:



- 2 Complete the fields in the Change Password dialog box.
- 3 Click on the **OK** button.

Result: The Board Password Changed Successfully dialog box displays.

Note: This means that Configuration Manager has written the password to the RLC's Flash memory.

- 4 Click on the **OK** button.
- 5 From the Menu Bar, choose Upload/Download → Save to Flash.

Result: Configuration Manager updates RLC's memory with the new password.

- 6 Restart the RLC.

Creating a backup configuration file

Create a backup copy of the RLC's configuration by downloading the configuration from flash memory to a text file on your administration PC. Nortel Networks recommends that you create a backup of your configuration file whenever you make configuration changes or after you perform a firmware upgrade.

Storing backup configuration files

The RLC is an extension of the telecommunications and data network. It is extremely important that you keep a backup copy of the RLC's configuration. If the RLC's Flash memory or configuration becomes corrupted or is lost, you can easily restore it.

Store the configuration file in a safe, secure location, such as on backup tape or other media that is stored offsite.

Nortel Networks recommends that you keep the backup files indefinitely.

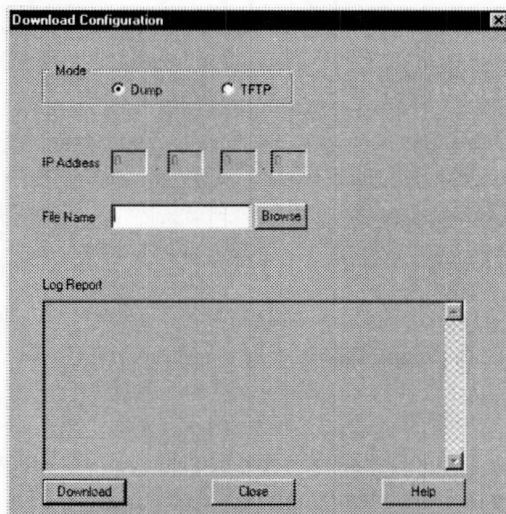
Getting there RLC → Configuration Manager

Creating the backup file

To create the backup file:

- 1 From the Menu Bar, choose Upload/Download → Download Configuration.

Result: The Download Configuration dialog box displays, similar to the following:



- 2 Choose the mode you want to use for the file transfer according to the following table:

IF you wish to save the configuration file to

the administration PC,
a different location on the IP
network,

THEN do the following:

Click on the **Dump** option button.

- 1 Click on the **TFTP** option button.

Result: This enables the IP Address fields.

- 2 Enter the IP address of the PC that you want to save the configuration file on.

- 3 Click on the **Browse** button and navigate to the folder where you want to keep the configuration text file.
- 4 Enter a name for the file in the File name field.

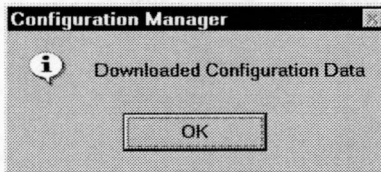
Note: This configuration file becomes your backup file, so ensure the file name is meaningful. The file name's extension must be .TXT.

- 5 Click on the **Download** button.

Result: The Download configuration dialog box closes, and the following message displays in the status bar at the bottom of the screen:

Downloading Config From Board

When the download is complete, the Downloaded Configuration Data dialog box displays, similar to the following:



- 6 Click on the **OK** button.

Note: Flash downloads to remote M39xx telephones can take twice as long compared to when these telephones are connected directly to a standard Nortel digital line card (XDLC).

Restoring the configuration

Restore the configuration to the RLC's Flash memory by uploading a configuration text file from a PC on the same network as the RLC. To do this, perform the upload over the IP network using the TFTP protocol.

Before you begin

Before you can upload the configuration file to the RLC, you must complete the following steps:

- 1 Start the TFTP server application.
- 2 Ensure that the TFTP base directory points to the location of the configuration file.

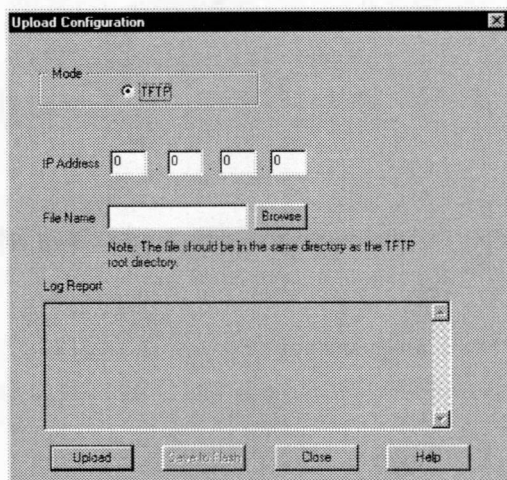
Getting there RLC → Configuration Manager

Uploading a configuration file over the IP network

To upload a configuration file over the IP network:

- 1 From the Menu Bar, choose → Upload/Download → Upload Configuration.

Result: The Upload Configuration dialog box displays, similar to the following:

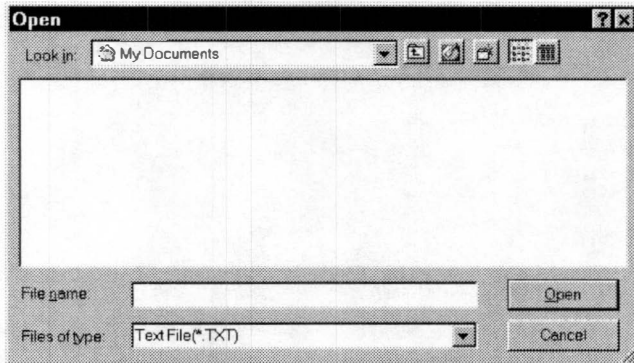


- 2 Enter the IP address of the TFTP server in the IP Address fields.

Note: Since the TFTP server application is running on your administration PC, this is the IP address of the administration PC.

- 3 Click on the **Browse** button.

Result: The Open dialog box displays, similar to the following:

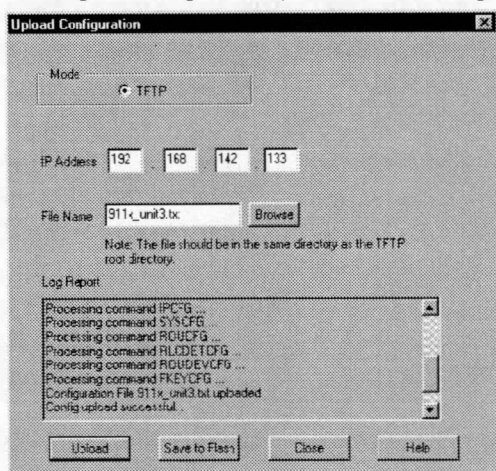


- 4 Ensure the Files of type drop down box shows Text File (*.TXT).
- 5 Navigate to the folder containing the configuration file.
- 6 Select the configuration file, and then click on the **Open** button.

Result: The Upload Configuration dialog box displays with the file you selected shown in the File Name field.

- 7 Click on the **Upload** button.

The middle of the Upload Configuration dialog box displays status messages relating to the upload. The following is an example.



CAUTION

Risk of incorrect operation due to partial configuration.

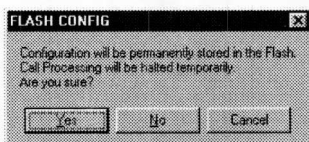
Do not interrupt the configuration upload. If you interrupt the configuration upload, this results in an incomplete configuration in the RLC's database.

If the configuration upload is interrupted, repeat this procedure immediately.

IF the upload was	THEN
successful,	the following message displays: CONFIG UPLOAD SUCCESSFUL... USE SAVECFG TO UPDATE FLASH. Proceed to step 8.
not successful,	the following message displays in the middle of the Upload Configuration dialog box: CONFIG UPLOAD FAILED For further instructions, refer to Chapter 8, "Troubleshooting".

- 8 On the Upload Configuration dialog box, click on the **Save to Flash** button.

Result: The FLASH CONFIG dialog box displays, similar to the following:



- 9 Click on the **Yes** button.

Result: The following message displays in the status bar at the bottom of the screen:

Saving to Flash in Progress

When the save is finished, the following message displays in the middle of the Upload Configuration dialog box:

CONFIGURATION IS UPDATED INTO FLASH...

- 10 Click on the **Close** button.
11 Restart the RLC.

Note: For instructions, refer to "Performing a system restart or shutdown" on page 143.

Display logs

The RLC keeps track of system performance through the maintenance of display logs. Each line, or display log, represents a separate action completed by the unit. Refer to Configuration Manager Help for a complete listing of all display logs and the condition indicated by each.

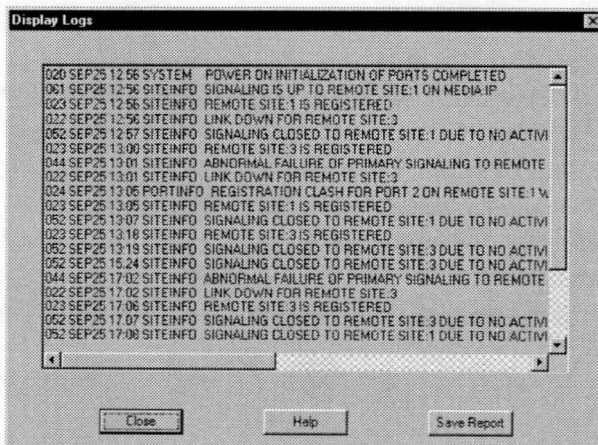
Use the display logs when troubleshooting system problems. Click on the **Save Report** button to print the display logs to a text file, or you can copy the information from the Display Logs window, and paste it into a text file.

Getting there RLC → Configuration Manager

Viewing display logs

From the Menu Bar, choose Alarms/Stats/Logs → Display Logs.

Result: You can view the RLC's display logs in a window similar to the following. You can use the scroll bar to browse through the logs.



Printing the display logs to a file

If you request technical support, your support representative can ask you to provide a copy of the logs. To recreate the log in a file on your administration PC, follow this procedure:

- 1 After displaying the logs using the procedure explained under "Viewing display logs" on page 208, click on the **Save Report** button on the Display Logs window.

Result: The Save As dialog box displays, similar to the following:



- 2 Navigate to the folder where you want to store the log file.
- 3 Enter a name for the configuration in the File name field.
- 4 Click on the **Save** button.

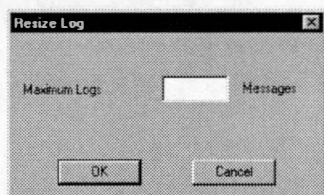
Result: Configuration Manager saves the logs to a text file in the location indicated in the Save As dialog box.

Changing the size of RLC logs

The RLC retains a maximum of 1000 display logs, each requiring one line of text. When the RLC's display logs reach 1000 lines, new display logs overwrite existing display logs on a first in, first out basis. If you want to change the number of display logs retained by the RLC:

- 1 From the Menu Bar, choose Alarms/Stats/Logs → Resize Logs.

Result: The Resize Log dialog box displays, similar to the following:



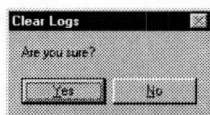
- Note:** "Maximum logs" refers to the number of text lines maintained in the RLC system log. The log holds a maximum of 1000 text lines, or the 1000 most recent display logs, when it shipped from the factory.
- 2 Enter the maximum number of display logs you want the RLC to keep in the Maximum Logs field.
 - 3 Click on the **OK** button.

Clearing logs

The RLC allows you to delete unneeded information by clearing the display logs that the RLC keeps. To discard or clear display logs that are no longer useful:

- 1 From the Menu Bar, choose the Alarms/Stats/Logs.

Result: The CLEAR LOGS dialog box displays, similar to the following:



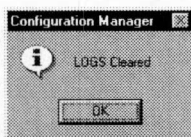
IF you select**THEN**

No,

the Clear logs dialog box closes and the logs remain as they are.

Yes,

- the RLC deletes its stored display logs.
- the LOGS cleared dialog box displays, similar to the following:



Click on the **OK** button.

Statistics screens

All statistics screens provided by the Alarms/Stats/Logs menu, function primarily to help you obtain information to provide to technical support personnel, upon request.

Getting there RLC → Configuration Manager

Trunk Connection Statistics

Trunk Connection Statistics show you the PSTN trunk usage for the selected remote site, similar to the following:

[illegible]

To display the Trunk Connection Statistics screen, refer to “Displaying the Trunk Connection Statistics screen”. To obtain the definitions for the statistics presented on the Trunk Connection Statistics screen, refer to “Trunk Connection Statistics field descriptions” on page 214.

Displaying the Trunk Connection Statistics screen

Choose Alarms/Stats/Logs → Trunk Connection Statistics from the Menu Bar to display the Trunk Connection Statistics screen.

Result: Configuration Manager gathers statistics from the RLC and displays the Trunk Connection Statistics screen, similar to the example on page 212.

IF you want to	THEN click
update the statistics with the latest information,	on the Refresh button.
create a text file containing these statistics,	on the Save to File button.
close the Trunk Connection Statistics screen,	on the Close button.
obtain descriptions of the statistics in the Trunk Connection Statistics screen,	on the Help button.

Trunk Connection Statistics field descriptions

The following table describes the statistics on the Trunk Connection Statistics screen:

Statistic	Description
Trunk Number	RLC - Identifies the Network Port number used for the call The third pair of numbers (the third item in the triplet) corresponds to the port on the RLC. 9150 - Identifies the ISDN BRI module and B-channel used for the call. 911x - Identifies the only trunk available to the remote unit with all zeroes.
Status	Identifies the current status of the trunk. Valid options are: Active, Idle.
Call Type	Identifies whether the call is a local call or a remote signaling call. Valid options are: Local, Signaling.
Remote ID	Identifies the remote unit involved in the call.
Called Number	Identifies the remote DN regardless of who initiated the call.
Start Time	Identifies the time that the last call on this trunk began.
Close Time	Identifies the time that the last call on this trunk ended. If the trunk is active, this statistic displays "NA".
Duration	Identifies the amount of time taken for the call.

Bandwidth Connection Statistics

Bandwidth Connection Statistics allow you to see how much bandwidth is actually being used. These statistics help you determine if you need to add more bandwidth on the PSTN or IP network connections. They show the amount of bandwidth all remote units connected to the logged-on RLC have available to them, similar to the following:

Remote Unit Number	Signaling Status	No of Voice Calls on IP	No of Voice Calls on PSTN	Used IP Bw	Used Trunk
1	ACTIVE	0	0	15.00	0.00
2	IDLE	0	0	0.00	0.00
3	IDLE	0	0	0.00	0.00
4	IDLE	0	0	0.00	0.00
5	IDLE	0	0	0.00	0.00
6	IDLE	0	0	0.00	0.00
7	IDLE	0	0	0.00	0.00
8	IDLE	0	0	0.00	0.00
9	IDLE	0	0	0.00	0.00
10	ACTIVE	0	0	15.00	0.00
13	IDLE	0	0	0.00	0.00
14	IDLE	0	0	0.00	0.00
15	IDLE	0	0	0.00	0.00
16	IDLE	0	0	0.00	0.00
17	IDLE	0	0	0.00	0.00

Refresh Save to File Close Print Help

To display the Bandwidth Connection Statistics screen, refer to “Displaying the Bandwidth Connection Statistics screen” on page 216. To obtain the definitions for the statistics presented on the Bandwidth Connection Statistics screen, refer to “Bandwidth Connection Statistics field descriptions” on page 217.

Displaying the Bandwidth Connection Statistics screen

Choose Alarms/Stats/Logs → BW Connection Statistics from the Menu Bar to display the Bandwidth Connection Statistics screen.

Result: Configuration Manager gathers statistics from the RLC and displays the Bandwidth Connection Statistics, similar to the example on page 215.

IF you want to	THEN click
update the statistics with the latest information,	on the Refresh button.
create a text file containing these statistics,	on the Save to File button.
close the Bandwidth Connection Statistics screen,	on the Close button.
obtain descriptions of the statistics in the Bandwidth Connection Statistics screen,	on the Help button.

Bandwidth Connection Statistics field descriptions

The following table describes the statistics on the Bandwidth Connection Statistics screen:

Statistic	Description
Remote Unit Number	Identifies the remote unit that initiated the call.
Signaling Status	Identifies whether a connection is up on this unit. Valid options are: Active, Idle
No of Voice Calls on IP	Identifies the number of calls in progress on this unit's IP connection.
No of Voice Calls on PSTN	Identifies the number of calls in progress on this unit's PSTN connection.
Used IP BW	Identifies the IP bandwidth in use on this unit.
Used Trunk BW	Identifies the PSTN bandwidth in use on this unit.
Total Up Trunk BW	Identifies the total PSTN bandwidth up and available to this unit.
IP QoS Status	Identifies the quality of service level on this unit's IP connection. Valid options are: Good, Bad.

Caller Info Statistics

Caller Info (Information) Statistics show you the types of calls being made (IP or PSTN) and how often QoS transitions occur. Use these statistics to help you determine if voice QoS on your IP network is stable. The Caller Info Statistics screen is similar to the following:

The screenshot shows a software window titled "Caller Info Statistics". It contains a table with the following columns: Connection ID, Remote ID, Current Media, Type, Priority, Call BW, Start Time, and Transitions to PSTN. The first two rows of data are visible:

Connection ID	Remote ID	Current Media	Type	Priority	Call BW	Start Time	Transitions to PSTN
97	1	IP	SIGNALING	IPONLY	16.00	07/03/2001	0
101	10	IP	SIGNALING	IPONLY	16.00	07/03/2001	0

Below the table is a horizontal scrollbar. At the bottom of the window are five buttons: Refresh, Save to File, Close, Reset, and Help.

To display the Caller Info Statistics screen, refer to “Displaying the Caller Info Statistics screen” on page 219. To obtain the definitions for the statistics presented on the Caller Info Statistics screen, refer to “Caller Info Statistics field descriptions” on page 220.

Displaying the Caller Info Statistics screen

Choose Alarms/Stats/Logs → Caller Info Statistics from the Menu Bar to display the Caller Info Statistics screen.

Result: Configuration Manager gathers statistics from the RLC and displays the Caller Info Statistics screen, similar to the example on page 218:

IF you want to	THEN click
update the statistics with the latest information,	on the Refresh button.
create a text file containing these statistics,	on the Save to File button.
close the Caller Info Statistics screen,	on the Close button.
obtain descriptions of the statistics in the Caller Info Statistics screen,	on the Help button.

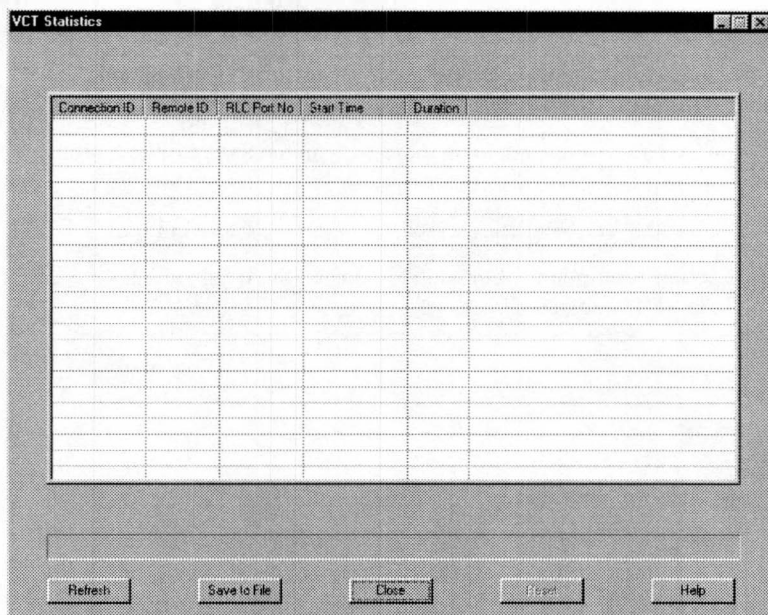
Caller Info Statistics field descriptions

The following table describes the statistics on the Caller Info Statistics screen:

Statistic	Description
Connection ID	Identifies the serial number of this call through the lifetime of the logged on unit.
Remote ID	Identifies the unit ID of the involved remote unit.
Current Media	Identifies whether the call took place over the PSTN or IP network.
Type	Identifies the type of call. Valid options are: Signaling, Voice, Local.
Priority	Identifies the priority setting of the involved trunk. Valid options are: PSTN Only, IP Only, High, or Normal.
Call BW	Identifies the amount of bandwidth used by the call.
Start Time	Identifies the time that the connection initiated.
Transitions to PSTN	Identifies the number of times the RLC moved the call to the PSTN.
Transitions to IP	Identifies the number of times the RLC moved the call to the IP network.
Last Transition to PSTN	Identifies the last time the RLC moved the call from the IP network to the PSTN.
Last Transition to IP	Identifies the last time the RLC moved the call from the PSTN to the IP network.

VCT Statistics

VCT (Voice Connection Table) Statistics provide information concerning certain properties of the voice connections that are active at the time that you request the statistics. Technical support personnel use these statistics for troubleshooting purposes. The VCT Statistics screen is similar to the following:



To display the VCT Statistics screen, refer to “Displaying the VCT Statistics screen” on page 222. To obtain the definitions for the statistics presented on the VCT Statistics screen, refer to “VCT Statistics field descriptions” on page 223.

Displaying the VCT Statistics screen

Choose Alarms/Stats/Logs → VCT from the Menu Bar to display the VCT Statistics screen:

Result: Configuration Manager gathers statistics from the RLC and displays the VCT Statistics screen, similar to the example on page 221.

IF you want to	THEN click
update the statistics with the latest information,	on the Refresh button.
create a text file containing these statistics,	on the Save to File button.
close the VCT Statistics screen,	on the Close button.
obtain descriptions of the statistics in the VCT Statistics screen,	on the Help button.

VCT Statistics field descriptions

The following table describes the statistics on the VCT Statistics screen:

Statistic	Description
Connection ID	Identifies the serial number of this call through the lifetime of the logged on unit.
Remote ID	Identifies the unit ID of the remote unit involved in the call.
RLC Port No	Identifies the port the call was processed through at the host site.
Start Time	Identifies the time and date when the call started.
Duration	Identifies how long the call lasted.

Hardware Statistics

Hardware Statistics provide information concerning the DSP modules that are installed on the logged-on RLC. Use these statistics to determine the module positions that are populated and the type of DSP modules present in the populated positions. The Hardware Statistics screen is similar to the following:

The screenshot shows a window titled "Hardware Statistics". Inside the window is a table with the following data:

Module No	Status	Module Type	Version
1	EQUIPPED	DSP_2TMS320LC549	
2	EQUIPPED	DSP_2TMS320LC549	
3	EQUIPPED	DSP_2TMS320LC549	
4	EQUIPPED	DSP_2TMS320LC549	

Below the table is a search bar and four buttons: Refresh, Save to File, Close, and Help.

To display the Hardware Statistics screen, refer to “Displaying the Hardware Statistics screen” on page 226. To obtain the definitions for the statistics presented on the Hardware Statistics screen, refer to “Hardware Statistics field descriptions” on page 227.

Information concerning the DSP application modules that are installed on the RLC also appears in the Startup Information dialog box. This information includes the following:

The column	contains the following information:
SLOTNO	the slot number occupied by the application module. Valid options are: 1, 2, 3, 4.
STATUS	whether the slot contains a functioning DSP application module. Valid options are: ■ EQUIPPED—a working DSP application module is in the slot ■ OUT SERVICE—a faulty application module is in the slot ■ UNEQUIPPED—no application module is in the slot
TYPE	the type of application module in the slot
VERSION	the version of application module in the slot

This dialog box displays as the result of a successful attempt to log on to a particular RLC. You can locate the information contained in the preceding table by using the scroll bar available in the System Information section of the dialog box. Refer to page 139 for further details.

Displaying the Hardware Statistics screen

Choose Alarms/Stats/Logs → Hardware Statistics from the Menu Bar to display the Hardware Statistics screen:

Result: Configuration Manager gathers statistics from the RLC and displays the Hardware Statistics screen, similar to the example on page 224.

IF you want to	THEN click
update the statistics with the latest information,	on the Refresh button.
create a text file containing these statistics,	on the Save to File button.
close the Hardware Statistics screen,	on the Close button.
obtain descriptions of the statistics in the Hardware Statistics screen,	on the Help button.

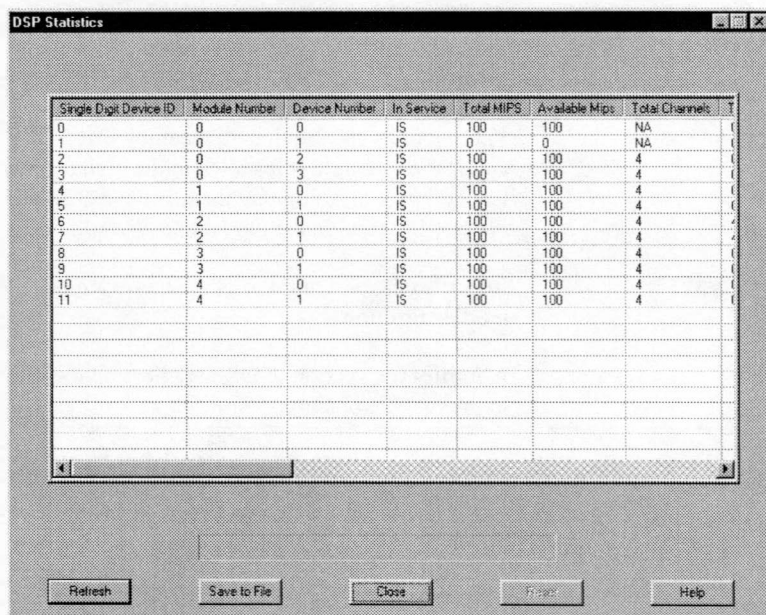
Hardware Statistics field descriptions

The following table describes the statistics on the Hardware Statistics screen:

Statistic	Description
Module No	Identifies the DSP application module's position on the RLC's motherboard.
Status	Identifies whether there is a functional DSP application module in the position identified in the Module No field. Valid options are: Equipped, meaning that a DSP application module is installed in the module position, and Unequipped, meaning that there is not a DSP application module installed in the module position.
Module Type	Identifies the part number of the hardware installed in the module position.
Version	Identifies the version of DSP application module installed in the module position.

Digital Signal Processor (DSP) Statistics

Digital Signal Processor (DSP) Statistics provide information about the DSP application modules installed on the logged-on RLC. Use this screen to determine the module positions that are populated, what type of DSP those positions contain, and the functionality provided by each module. The DSP Statistics screen is similar to the following:



The screenshot shows a window titled "DSP Statistics" with a table of DSP application modules. The table has seven columns: Single Digit Device ID, Module Number, Device Number, In Service, Total MIPS, Available MIPS, and Total Channels. The data is as follows:

Single Digit Device ID	Module Number	Device Number	In Service	Total MIPS	Available MIPS	Total Channels
0	0	0	IS	100	100	NA
1	0	1	IS	0	0	NA
2	0	2	IS	100	100	4
3	0	3	IS	100	100	4
4	1	0	IS	100	100	4
5	1	1	IS	100	100	4
6	2	0	IS	100	100	4
7	2	1	IS	100	100	4
8	3	0	IS	100	100	4
9	3	1	IS	100	100	4
10	4	0	IS	100	100	4
11	4	1	IS	100	100	4

Below the table are five buttons: Refresh, Save to File, Close, Print, and Help.

To display the DSP Statistics screen, refer to “Displaying the DSP Statistics screen” on page 229. To obtain the definitions for the statistics presented on the DSP Statistics screen, refer to “DSP Statistics field descriptions” on page 230.

Displaying the DSP Statistics screen

Choose Alarms/Stats/Logs → DSP Statistics from the Menu Bar to display the DSP Statistics screen:

Result: Configuration Manager gathers statistics from the RLC and displays the DSP Statistics screen, similar to the example on page 228.

IF you want to	THEN click
update the statistics with the latest information,	on the Refresh button.
create a text file containing these statistics,	on the Save to File button.
close the DSP Statistics screen,	on the Close button.
obtain descriptions of the statistics in the DSP Statistics screen,	on the Help button.

DSP Statistics field descriptions

The following table describes the statistics on the DSP Statistics screen:

Statistic	Description
Single Digit Device ID	Identifies an internal sequence number for indexing this DSP device among all others on the RLC.
Module Number	Identifies this DSP Application Module's module number on the RLC. Valid options are: 0, 1, 2, 3, 4.
Device Number	Identifies the DSP device that processed the call.
In Service	Identifies any voice channels operating on this DSP application module.
Total MIPS	Identifies the total millions of instructions per second (MIPS) capacity for this DSP device.
Available Mips	Identifies the millions of instructions per second (MIPS) currently available on this DSP device.
Total Channels	Identifies the total channel capacity for this DSP device.
Total Voice Channels	Identifies the total voice channel capacity for this DSP device.
Available Voice Channels	Identifies the number of unused voice channels on this DSP device.
Total Modem Channels	Identifies the number of channels on this DSP device that can transmit modem calls.

Statistic	Description
Available Modem Channels	Identifies the number of unused channels on this DSP that can transmit modem calls.
Total Flex Channels	Identifies the number of channels on this DSP that can provide multiple functionalities.
Available Flex Channels	Identifies the number of channels on this DSP currently available to provide multiple functionalities.
Total Tones Channels	Identifies the number of channels on this DSP that can transmit tones.
Total Reserved Channels	Identifies the number of special purpose channels on this DSP reserved for internal use.
Name	Identifies the name of the DSP load, that is, the combination of DSP algorithms, on the DSP module.

Ethernet Interface Statistics

Ethernet Interface Statistics provide information about the connection between the IP network and the logged-on RLC that is achieved over the RLC's Ethernet interface. The Ethernet Interface Statistics screen is similar to the following:

Ethernet Interface Statistics

Channel	LANDrv	Admin	Oper	IfcType	IfcNo	MTUlen	Speed	IN - Octets	UPkts	MPkts	Disc	Err
1	POWERQ	1	1	6	1	1500	100	153650	106	156	17	0
2	UNKNOWN	0	0	0	0	0	0	0	0	0	0	0

To display the Ethernet Interface Statistics screen, refer to “Displaying the Ethernet Interface Statistics screen” on page 233. To obtain the definitions for the statistics presented on the Ethernet Interface Statistics screen, refer to “Ethernet Interface Statistics field descriptions” on page 234.

Displaying the Ethernet Interface Statistics screen

Choose Alarms/Stats/Logs → Ethernet Interface Statistics from the Menu Bar to display the Ethernet Interface Statistics screen.

Result: Configuration Manager gathers statistics from the RLC and displays the Ethernet Interface Statistics screen, similar to the example on page 232.

IF you want to	THEN click
update the statistics with the latest information,	on the Refresh button.
create a text file containing these statistics,	on the Save to File button.
close the Ethernet Interface Statistics screen,	on the Close button.
obtain descriptions of the statistics in the Ethernet Interface Statistics screen,	on the Help button.

Ethernet Interface Statistics field descriptions

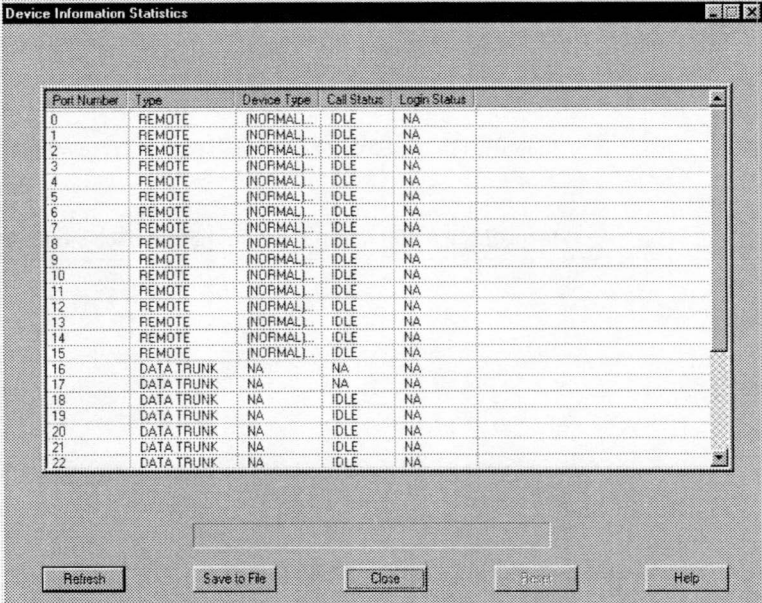
The following table describes the statistics on the Ethernet Interface Statistics screen:

Statistic	Description
Channel	Identifies the Ethernet device that the statistics on that line apply to. Valid options are: 1, 2.
LAN Drv	Identifies the LAN driver used by the call.
Admin	Identifies the desired state of the port.
Oper	Identifies the actual state of the port.
IfcType	Identifies the interface type used by the call.
IfcNo	Identifies the Ethernet interface used by the call. Valid options are: 0 (ELAN), 1 (CLAN).
MTUlen	Identifies the Maximum Transmission Unit for this interface.
Speed	Identifies the data rate of this interface.
In - Octet	Identifies the number of inbound bytes.
UPkts	Identifies the number of inbound packets sent only to this recipient.
MPkts	Identifies the number of inbound packets sent to multiple recipients.
Disc	Identifies the number of packets discarded by the interface.
Err	Identifies the number of error packets received by the interface.
Out - Octet	Identifies the number of outbound bytes.
UPkts	Identifies the number of outbound packets sent only to this recipient.

Statistic	Description
MPkts	Identifies the number of outbound packets sent to multiple recipients.
Disc	Identifies the number of outbound packets discarded by the interface due to resource problems.
Err	Identifies the number of outbound packets discarded due to errors.
QLen	Identifies the number of bytes in the interface's outbound queue.

Device Information Statistics

Device Information Statistics provide information about the device connected to each port of the logged-on RLC, similar to the following:



The screenshot shows a window titled "Device Information Statistics" with a table of port information. The table has five columns: Port Number, Type, Device Type, Call Status, and Login Status. The data is as follows:

Port Number	Type	Device Type	Call Status	Login Status
0	REMOTE	(NORMAL)	IDLE	NA
1	REMOTE	(NORMAL)	IDLE	NA
2	REMOTE	(NORMAL)	IDLE	NA
3	REMOTE	(NORMAL)	IDLE	NA
4	REMOTE	(NORMAL)	IDLE	NA
5	REMOTE	(NORMAL)	IDLE	NA
6	REMOTE	(NORMAL)	IDLE	NA
7	REMOTE	(NORMAL)	IDLE	NA
8	REMOTE	(NORMAL)	IDLE	NA
9	REMOTE	(NORMAL)	IDLE	NA
10	REMOTE	(NORMAL)	IDLE	NA
11	REMOTE	(NORMAL)	IDLE	NA
12	REMOTE	(NORMAL)	IDLE	NA
13	REMOTE	(NORMAL)	IDLE	NA
14	REMOTE	(NORMAL)	IDLE	NA
15	REMOTE	(NORMAL)	IDLE	NA
16	DATA TRUNK	NA	NA	NA
17	DATA TRUNK	NA	NA	NA
18	DATA TRUNK	NA	IDLE	NA
19	DATA TRUNK	NA	IDLE	NA
20	DATA TRUNK	NA	IDLE	NA
21	DATA TRUNK	NA	IDLE	NA
22	DATA TRUNK	NA	IDLE	NA

Below the table, there is a search bar and five buttons: Refresh, Save to File, Close, Print, and Help.

To display the Device Information Statistics screen, refer to “Displaying the Device Information Statistics screen” on page 237. To obtain the definitions for the statistics presented on the Device Information Statistics screen, refer to “Device Information Statistics field descriptions” on page 238.

Displaying the Device Information Statistics screen

Choose Alarms/Stats/Logs → Device Information from the Menu Bar to display the Device Information Statistics screen.

Result: Configuration Manager gathers statistics from the RLC and displays the Device Information Statistics screen, similar to the example on page 236.

IF you want to	THEN click
update the statistics with the latest information,	on the Refresh button.
create a text file containing these statistics,	on the Save to File button.
close the Device Information Statistics screen,	on the Close button.
obtain descriptions of the statistics in the Device Information Statistics screen,	on the Help button.

Device Information Statistics field descriptions

The following table describes the information on the Device Information Statistics screen:

Statistic	Description
Port Number	Identifies the RLC Port that the statistics on that line of the table apply to.
Type	Identifies the kind of trunk established to the port identified by the Port Number statistic. Valid options are: Data Trunk, Remote, Local TCM.
Device Type	Identifies whether the device connected to the port identified by the Port Number statistic is part of an ACD queue. Valid options are: ACD, Normal, NA.
Call Status	Identifies whether there is a call active on the port identified by the Port Number statistic. Valid options are: Active, Idle, NA.
Login Status	Identifies whether there is a user logged on to the port identified by the Port Number statistic. Valid options are: Logged In, NA.

Network Statistics screen

Network Statistics allow you to see the performance over the last 24 hours of the remote units connected to the logged-on RLC. Use these statistics to identify periods when other network activity can adversely affect Remote Office system performance. This screen shows remote unit performance in terms of the transmission and reception of frames and packets, similar to the following.

Network Statistics

Remote Unit Number = 1 IP Address : 192.168.143.101

Hour	Tx Frames	Rx Frames	Rx Error	Rx Dropped	Error %	BroadCast Packet	Tx UCastPkt	Tx DiscPkt	F
0	0	0	0	0	0.00	1	1291	0	
1	0	0	0	0	0.00	0	420	0	
2	0	0	0	0	0.00	0	464	0	
3	0	0	0	0	0.00	0	325	0	
4	0	0	0	0	0.00	0	319	0	
5	0	0	0	0	0.00	0	8821	0	
6	50	174	0	0	0.00	0	30002	0	
7	0	0	0	0	0.00	0	326	0	
8	0	0	0	0	0.00	0	326	0	
9	0	0	0	0	0.00	0	326	0	
10	0	0	0	0	0.00	0	329	0	
11	0	0	0	0	0.00	0	331	0	
12	0	0	0	0	0.00	0	330	0	
13	0	0	0	0	0.00	0	330	0	
14	0	0	0	0	0.00	0	327	0	
15	0	0	0	0	0.00	2	358	0	
16	0	0	0	0	0.00	0	329	0	
17	0	0	0	0	0.00	0	328	0	
18	0	0	0	0	0.00	0	328	0	
19	0	0	0	0	0.00	0	336	0	
20	0	0	0	0	0.00	0	329	0	
21	0	0	0	0	0.00	0	328	0	

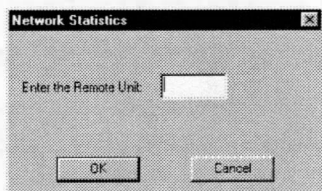
Refresh Save to File Close Help

To display the Network Statistics screen, refer to “Displaying the Network Statistics screen” on page 240. To obtain the definitions for the statistics presented on the Network Statistics screen, refer to “Network Statistics field descriptions” on page 241.

Displaying the Network Statistics screen

- 1 Choose Alarms/Stats/Logs → Network Statistics from the Menu Bar to display the Network Statistics screen.

Result: Configuration Manager prompts you for the unit ID of the remote unit that you want to check Network Statistics for, similar to the following:



- 2 Enter the Unit ID.
- 3 Click on the **OK** button.

Result: The Network Statistics screen displays, similar to the example on page 239.

IF you want to	THEN click
update the statistics with the latest information,	on the Refresh button.
create a text file containing these statistics,	on the Save to File button.
close the Network Statistics screen,	on the Close button.
obtain descriptions of the statistics in the Network Statistics screen,	on the Help button.

Network Statistics field descriptions

The following table describes the information on the Network Statistics screen:

Statistic	Description
Hour	Identifies the hour that the statistics on that line apply to. These numbers refer to the most recent 24 hours, such that "1" refers to one hour ago, "2" refers to two hours ago, and so on.
Tx Frames	Identifies the number of frames transmitted in the given hour.
Rx Frames	Identifies the number of frames received in the given hour.
Rx Error	Identifies the number of frames received in the given hour with an error.
Rx Dropped	Identifies the number of received frames that the Remote Office system dropped in the given hour.
Error %	Identifies the percentage of frames received in the given hour with an error.
BroadCast Packet	Identifies the number of packets broadcast, or sent to all addresses on the network, by this unit in the given hour.
Tx UCastPkt	Identifies the number of packets unicast, or sent to one specific address, by this unit in the given hour.
Tx DiscPkt	Identifies the number of packets discarded by this unit in the given hour.
Rx MultiPkt	Identifies the number of packets received by this unit that were sent to multiple addresses in the given hour.
Rx UCastPkt	Identifies the number of packets received by this unit that were sent only to this unit in the given hour.
Rx DiscPkt	Identifies the number of received packets that were discarded by this unit in the given hour.

PSTN Error Statistics screen

PSTN Error Statistics allow you to see the PSTN performance, in terms of signaling errors, of remote units connected to the logged-on RLC. Use these statistics to indicate the effectiveness of your connection to the PSTN. The table displays error totals for all active PSTN calls from the specified remote unit, similar to the following.

PSTN Error Statistics

Remote Unit Number = 1
Total Transmitter Underruns : 0 Total Receive Overflows : 0 Total Interrupt overflow count : 0

Channel Number	Receive Buffer Allocation Failures	Frame Length Violations	CRC Errors	Unknown Receive Errors
16	0	0	70	70

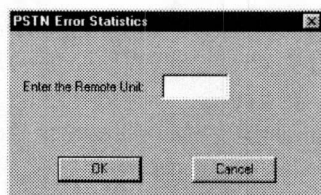
Refresh Save to File Close Reset Help

Note: PSTN Error Statistics are only available for Remote Office 9150 units.

Displaying the PSTN Error Statistics screen

- 1 Choose Alarms/Stats/Logs → PSTN Error Statistics from the Menu Bar to display the PSTN Error Statistics screen.

Result: Configuration Manager prompts you for the unit ID of the remote unit that you want to check PSTN Error Statistics for, similar to the following:



- 2 Enter the Unit ID.
- 3 Click on the **OK** button.

Result: The PSTN Error Statistics screen displays, similar to the example on page 242.

IF you want to	THEN click on the
update the statistics by adding PSTN error information that occurred since your original request,	Refresh button.
create a text file containing these statistics,	Save to File button.
close the PSTN Error Statistics screen,	Close button.
begin collecting new statistics,	Reset button.
obtain descriptions of the statistics in the PSTN Error Statistics screen,	Help button.

PSTN Error Statistics field descriptions

The following table describes the information on the PSTN Error Statistics screen:

Statistic	Description
Channel Number	Identifies the channel that the statistics on that line apply to.
Receive Buffer Allocation Failures	Identifies the number of times since the statistics were last reset that there was an error in the allocation of a packet to the receive buffer.
Frame Length Violations	Identifies the number of times since the statistics were last reset that a frame contained too many packets.
CRC Errors	Identifies the number of times since the statistics were last reset that the cyclic redundancy check (CRC) bits did not match.
Unknown Receive Errors	Identifies the number of times since the statistics were last reset that a receive error that is not otherwise classified in this display occurred.
ITE Frame Length Violations	Identifies the number of bits in the ITE frame since the statistics were last reset.
ITE Transmitter Underruns	Identifies the number of times since the statistics were last reset that the ITE transmitter.
ITE Receive Busy Errors	Identifies the number of times since the last reset.

Verifying the firmware and software version

This section describes how to determine the version of firmware and software currently installed.

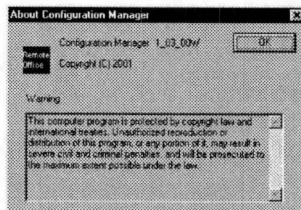
Before you perform a firmware or software upgrade, you should determine what version is currently installed. This ensures that you do not replace the installed firmware or software with an older version.

Verifying the software version

To verify the software version on your RLC:

- 1 From the Menu Bar, choose Help → About Configuration Manager.

Result: The About Configuration Manager dialog box displays, similar to the following:



- 2 Review the About Configuration Manager dialog box. This identifies the version of software installed on the unit.
- 3 Click on the **OK** button.

Verifying the firmware version

To verify the firmware version on your RLC:

- 1 From the Menu Bar, choose System Information → System Data.
- 2 The System Configuration Details dialog box displays, similar to the following:

SLOTRNO	STATUS	TYPE	VERSION
1	EQUIPPED	DSP_27M332LC549	
2	EQUIPPED	DSP_27M332LC549	
3	EQUIPPED	DSP_27M332LC549	
4	EQUIPPED	DSP_27M332LC549	

- 3 Review the Unit Version box. This identifies the version of firmware installed on the unit.
- 4 Click on the **Close** button.

Determining the current firmware and software versions

To determine what the current firmware and software versions are, refer to the *Remote Office and RLC Release Notes* (NTP 555-8421-102).

Obtaining the latest upgrade file

If you need to upgrade the firmware or software, you can obtain the latest upgrade files by clicking on the Customer Support and Software Distribution links at the following website:

www.nortelnetworks.com

Nortel Networks provides upgrade files in self-extracting executable files. You must extract the upgrade files before you can perform the upgrade.

Types of upgrades

You can perform the following types of upgrades for your RLC:

- Configuration Manager software upgrade
You use Configuration Manager software to configure or administer the RLC.
- firmware upgrade for the RLC motherboard
The firmware contains the code necessary for operating the RLC.

Note: This includes any firmware updates that have been made for DSP application modules.

Downloading the upgrade file

To download the upgrade file:

- 1 With your web browser, connect to the Nortel Networks website at:
www.nortelnetworks.com
- 2 Click on the Customer Support and Software Distribution links.
- 3 Locate the software and firmware you need.
- 4 Download the files into a temporary location on your PC.
- 5 Double-click on the **.exe** file to extract the files into a temporary location on your PC.

Performing a firmware upgrade

This section describes how to perform a firmware upgrade on your RLC. You perform the upgrade over the IP network using the TFTP protocol.

You must have a TFTP server application running on the administration PC. Ensure that the TFTP server's base directory points to the directory that contains the upgrade files.

To ensure that the RLC and Remote Office units do not experience communication problems during, or after the firmware upgrade, Nortel Networks recommends that you perform the upgrades as follows:

- 1 Create backup files for the Remote Office 9150, 911x, and IP Adapter units and RLC configurations. Refer to "Creating a backup configuration file" in the Nortel Networks Installation and Administration Guide for the specific product.
- 2 Upgrade the Configuration Manager software on the administration PC.
- 3 Disable the PBX slot where the RLC is installed.
- 4 Upgrade the RLC firmware.
- 5 Upgrade the Remote Office units - 9150, 911x, and IP Adapter firmware.
- 6 Remote Office 9150 units only - Upgrade the BRI module firmware for each BRI module.
- 7 Restart the RLC.
- 8 Restart all units.
- 9 Re-enable the RLC slot.

Note: The Remote Office 9150 unit's BRI module firmware must only be upgraded after the Remote Office 9150 unit's firmware is at the desired compatible level.

When to perform a firmware upgrade

Perform a firmware upgrade if you have determined that you are using out-of-date firmware. For instructions on determining if you need to perform an upgrade, refer to “Verifying the firmware and software version” on page 245.

ATTENTION

The protocol for communication between the RLC and the Remote Office units requires that they be running the same version in order for them to communicate with each other.

About firmware upgrades and configuration files

Each time you perform a firmware upgrade, the configuration database also converts (if necessary) to a format that is compatible with the new firmware. The conversion does not effect configuration settings.

Nortel Networks recommends that each time you perform a firmware upgrade, that you first create a backup copy of the converted configuration file and store it in a safe secure location.

Before you begin

It is important to complete the following steps before performing a firmware upgrade:

- 1 Obtain the firmware upgrade from Nortel Networks.
- 2 Extract the upgrade files from the file you received from Nortel Networks.
- 3 Start the TFTP server application.
- 4 Ensure the TFTP base directory reflects the directory where the firmware upgrade file you want to use resides.

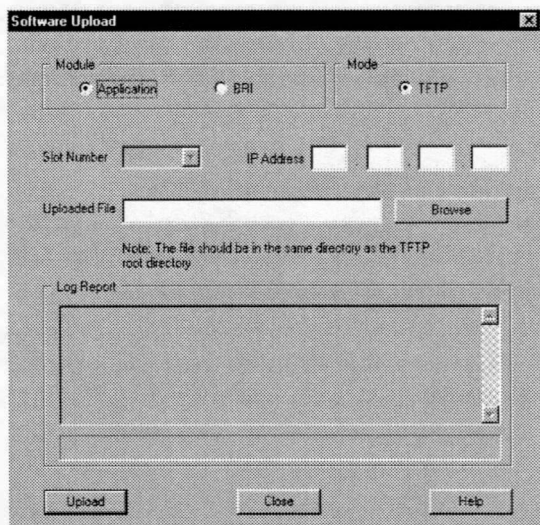
Getting there RLC → Configuration Manager

Upgrading the RLC firmware

To upgrade the RLC firmware:

- 1 From the Menu Bar, choose Upload/Download → Upload S/W.

Result: The Software Upload dialog box displays, similar to the following:



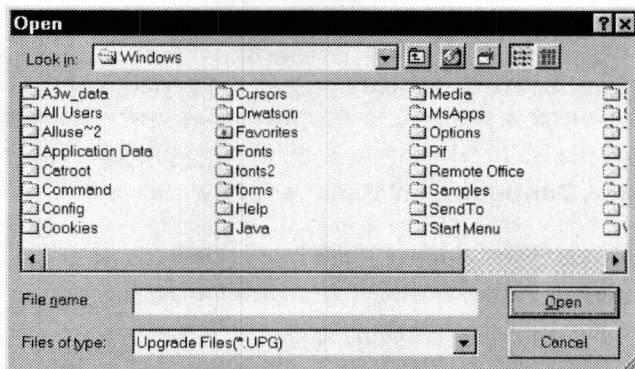
The image shows a 'Software Upload' dialog box with a title bar and a close button. It contains two sections: 'Module' and 'Mode'. The 'Module' section has two radio buttons: 'Application' (selected) and 'BRI'. The 'Mode' section has one radio button: 'TFTP'. Below these are fields for 'Slot Number' (a dropdown menu), 'IP Address' (four text boxes), and 'Uploaded File' (a text box with a 'Browse' button). A note states: 'Note: The file should be in the same directory as the TFTP root directory'. Below the note is a 'Log Report' section with a large text area and a 'Log' button. At the bottom are three buttons: 'Upload', 'Close', and 'Help'.

- 2 In the Module section, click on the **Application** option button.
- 3 Enter the IP address of the TFTP server in the IP Address fields.

Note: Since the TFTP server application runs on your administration PC, this is the IP address of the PC.

- 4 Click on the **Browse** button.

Result: The Open dialog box displays, similar to the following:



- 5 Ensure the Files of type drop down box shows Upgrade Files (*.UPG).
- 6 Navigate to the folder where the firmware file is located.
- 7 Select the file, and then click on the **Open** button.

Example: Select rlc-100.upg, and then click on the **Open** button.

Result: The Software Upload dialog box reappears. The file you selected is shown in the Uploaded File field.

- 8 Click on the **Upload** button.

Wait until the file uploads completely before entering any other commands. The Log Report window displays a confirmation message when the upgrade is completed.

- 9 Restart the RLC.

Performing a software upgrade

Perform a software upgrade if you have determined that you are using out-of-date software. For instructions on determining if you need to perform an upgrade, refer to “Verifying the firmware and software version” on page 245.

Upgrading the Configuration Manager software

To upgrade the Configuration Manager software:

- 1 Navigate to the directory that contains the upgrade files you extracted.
- 2 Double-click on the **setup.exe** file.
- 3 Follow the prompts on screen.

ATTENTION

Do not ignore any warning messages the InstallShield displays about versions of files (such as DLL files) that already exist on your PC. If you overwrite these files, you may inadvertently cause other applications on your PC to stop working.

Result: The InstallShield installs the software, overwriting the previous version.

Chapter 8

Troubleshooting

In this chapter

Before you begin	254
Reach Line Card LEDs	255
Network connectivity	258
Software problems	264
QoS testing	266
Using Configuration Manager PING	268
Responding to a catastrophic failure	271
Repair and warranty information	272

Before you begin

The questions listed in this section can help you determine the proper course of action for addressing your problem.

Identifying why a problem occurred

Before you begin, ask yourself the questions listed in the following table:

Question	IF you answered	THEN do the following steps
Is this a new installation?	yes	Perform troubleshooting in the sequence presented in this chapter.
	no	Answer the next question.
Did the RLC work, then suddenly stop working?	yes	Answer the next question.
	no	Perform troubleshooting in the sequence presented in this chapter.
Did you modify the configuration or change any hardware components?	yes	Verify that changes were made correctly. Check the hardware components to ensure they are working correctly. Perform troubleshooting for the specific component the problem appears in.
	no	Contact your telecom or data network administrator. There may be a problem with the network.

Reach Line Card LEDs

The Reach Line Card (RLC) LEDs give you an indication of the line card's general health. When you reset your RLC, the LEDs should behave as follows:

- The Maintenance LED should perform as follows upon card insertion:
 - light up solid
 - flash three times after completing its self-test

Note: The self-test takes approximately 60 seconds.

- go off after the host PBX enables the RLC

Note: During normal operation of the RLC, the Maintenance LED should remain off.

- The remaining LEDs flash when there is network activity.

What to do if the LEDs do not display correctly

The following table describes what to do if the LEDs do not display correctly:

Symptom	What to do
The Maintenance LED did not flash three times during the power-up cycle.	1 Reset the RLC. Watch the Maintenance LED again. Approximately 60 seconds pass before it flashes. 2 If the Maintenance LED still does not flash, contact your Nortel Networks distributor. There may be a hardware problem.
The Maintenance LED is lit after a successful self-test.	1 Check to see if the slot is enabled on the host PBX. 2 If other LEDs are not lit or flashing, did the Maintenance LED ever light? If not, contact your Nortel Networks distributor. There may be a hardware problem. 3 Ensure that the RLC is properly seated in its slot and is properly inserted into the backplane. If the Maintenance LED remains lit, contact your Nortel Networks distributor. There may be a hardware problem.
The Maintenance LED is flashing.	The power-up self-test failed. Contact your Nortel Networks distributor. There may be a hardware problem.
No LEDs are lit on the RLC.	1 Ensure that the slot the RLC resides in has power applied. 2 Ensure that the RLC is properly seated in its slot. If the RLC is properly seated in its slot and no LEDs light, contact your Nortel Networks distributor. There may be a hardware problem.

Symptom

The Ethernet COLL LED is lit solid.

What to do

Network collisions are bound to occur and are normal. However, if the Ethernet COLL LED is lit solid, complete the following steps:

- 1** Check the physical network connection.
- 2** Verify that the RLC can be PINGed.
- 3** Check the network configuration (such as routing, traffic load, and so on). Adjust the network configuration, if required.
- 4** There should be no broadcast or multicast activity on the telephony LAN (TLAN). Interconnect a hub and a network analyzer to the TLAN and monitor for such activity. Identify the source(s) and isolate them from the TLAN.

Network connectivity

This section identifies some problems that can occur on the network, and describes what to do to resolve them.

Symptom descriptions

If you are not able to establish or maintain data network connectivity, perform troubleshooting as described in the following table:

Symptom	What to do
You cannot establish a connection from your administration PC to the RLC.	1 Ensure that you entered the IP address correctly when trying to establish the connection.
	2 Ensure that you entered the logon name and password correctly when trying to establish the connection.
	3 Ensure the RLC's IP address, network mask, and default gateway are configured correctly on the RLC.
	4 PING the RLC.
	5 PING the gateway.
	6 If the PING still does not work, contact your data network administrator.

Symptom

10060 TELNET CONNECTION FAILED appears when attempting to connect to the RLC.

What to do

- 1 Ensure that you entered the IP address correctly when trying to establish the connection.
- 2 Ensure that you entered the logon name and password correctly when trying to establish the connection.
- 3 Ensure that no one is already logged on to the RLC.
- 4 Verify that the Ethernet cable is connected at both ends (RLC and network hub).
- 5 Check the Ethernet cable and ensure it is good.
- 6 Ensure the RLC is properly seated in its slot.
- 7 Verify that the IP address, subnet mask and gateway are all correct on the RLC.
- 8 PING the RLC.
- 9 If the RLC does not respond, PING the RLC's gateway to see if it responds.
- 10 If the gateway does not respond, PING a known good device on the RLC's network.
- 11 If steps 9 and 10 work, but step 8 did not, there may be a gateway configuration error. Check the unit's IP Configuration property sheet.
- 12 If the problem still exists, contact your Nortel Networks distributor. There may be a hardware problem.

Symptom	What to do
SERIAL CONNECTION FAILED appears when attempting to connect to the RLC.	1 Ensure that you entered the logon name and password correctly when trying to establish the connection. 2 Ensure that someone is not already logged on to the RLC. 3 Ensure the RLC is properly seated in its slot. 4 Reseat the RLC. 5 Ensure you specified the correct COM port when attempting the connection. 6 Verify that no other applications on the administration PC are using the COM port. 7 Check the serial cable connection to ensure it is good. 8 Using a breakout box, verify that the COM port is active. 9 If the problem still exists, contact your Nortel Networks distributor. There might be a hardware problem.
The RLC does not send or receive Ethernet traffic.	1 Ensure the RLC is seated in its slot properly and connected to the backplane. 2 Check the Ethernet cable between the RLC and the network and ensure it is good. 3 Ensure the Ethernet cable is connected. 4 If the RLC still does not send or receive traffic, contact your data network administrator. 5 Data network administrator: Ensure other network devices are configured to allow traffic to and from the RLC.

Symptom	What to do
An attempt to log off from the RLC does not work.	It is possible that the administration PC and the RLC have lost communication with one another. Close Configuration Manager, then restart it.
The RLC cannot establish a connection with the remote unit.	IP or PSTN installations: 1 Verify security authentication configuration and ensure that it matches at both ends. (For example, if using security identifier, ensure that the inbound and outbound security identifiers are correctly configured at each end.) 2 Ensure that the unit IDs are configured correctly at each end. An incorrect unit ID causes security authentication to fail. 3 Verify that the PSTN and IP networks are operational (up and running) as appropriate to your location. 4 Ensure that the RLC is enabled on the host PBX.

Symptom**What to do**

The RLC cannot establish a connection with the remote unit. (continued)

Additional steps for IP-only installations:

- 1** Confirm that the RLC's IP address and PSTN number are correctly configured on the remote unit. Also confirm that correct remote unit configuration exists at the host site.
- 2** Use the PING option in Configuration Manager to PING the remote unit. For instructions, refer to "Performing a Configuration Manager PING," on page 268.
- 3** If the remote unit does not respond, check the network configuration (such as, routing, traffic load, and so on). Adjust the network configuration, if required.

Additional steps for PSTN only installations:

- 1** Verify that network ports are configured on the host PBX, one for each BRI channel that is to provide remote connectivity.
- 2** Verify that the 9150 PSTN telephone number is configured correctly on both the Remote Connection Configuration property sheet (refer to "Remote Connection Configuration" on page 171) and the BRI Configuration property sheet (refer to "Configuring BRI Trunks" in the Remote Office 9150 Installation and Administration Guide NTP 555-8421-215).

Note: This is the same telephone number configured on both property sheets.

Symptom**What to do**

The RLC cannot establish a connection with the remote unit. (continued)

- 3** Verify that the network port PSTN telephone number is configured correctly on both the Network Port Configuration window of the RLC Port Configuration property sheet (refer to "Configuring an RLC port" on page 164) and "Configuring the RLC Connection information" in the Remote Office 9150 Installation and Administration Guide NTP 555-8421-215).

Note: This is the same telephone number configured on both property sheets.

Software problems

This section identifies some problems that can occur with the Configuration Manager software, and describes what to do to resolve them.

Symptom descriptions

If you are not able to complete a task with Configuration Manager, perform troubleshooting as described in the following table:

Symptom	What to do
The Configuration Manager software installation fails.	Ensure that you close all background applications, including anti-virus checking software before performing the installation.
When performing one of the following by TFTP, ERROR: FILE OPEN FAILED displays: ■ configuration upload ■ RLC firmware upgrade	1 Ensure the TFTP server application is installed and running on your administration PC. 2 Ensure the file you are trying to upload is present in the target directory. That is, either in the TFTP directory, or in the directory that is specified as the base directory in the TFTP server application. 3 Review messages displayed by the TFTP server application for clues. 4 Ping the remote unit to verify that network connectivity exists.
CONFIG UPLOAD FAILED when attempting to perform a configuration upload by TFTP.	1 Ensure that you selected an appropriate file. That is, ensure that the file you attempted to upload is an RLC configuration file.

Symptom	What to do
CONFIG UPLOAD FAILED when attempting to perform a configuration upload by TFTP. (continued)	2 Ensure that the configuration file you are attempting to upload is compatible with current RLC firmware. 3 Perform the configuration upload using a previous configuration file, if necessary. Note: Each time you perform a RLC firmware upgrade, you should also create a backup of the configuration. The configuration database format in the RLC is dependent on the version of firmware installed on the RLC. If you recently downgraded to a previous version of RLC firmware, you may also need to revert to a previous configuration format.
System not responding appears when working with Configuration Manager.	It is possible that communication has been lost between the administration PC and the remote unit. Close Configuration Manager, and then restart it.
Nothing happens when attempting to log off from the RLC.	It is possible that communication has been lost between the administration PC and the node you were logged on to. Close Configuration Manager, and then restart it.

Display Logs definitions

You can locate Display Logs definitions in Configuration Manager Help.

QoS testing

This section identifies problems that can occur during Quality of Service (QoS) testing when using IP connectivity as the main method of connectivity, with PSTN connectivity for QoS transition. This section also describes what to do to resolve the problem.

Symptom descriptions

If the Remote Office system does not make the transition to the PSTN connection when you disconnect the Ethernet cable (or the network goes down), perform troubleshooting as described in the following table:

Symptom	What to do
The connection does not transfer from the IP network to the PSTN when the Ethernet connection is broken.	1 Ensure that you selected PSTN:Status:Enable on the Remote Connection Configuration property sheet for the connection in question. ■ Ensure that the PSTN number of the remote unit is entered in the PSTN Number field on the same property sheet. ■ Ensure that the port number of the Dedicated Network Port is entered in the Dedicated PSTN n/w Port field on the same property sheet. 2 Ensure that the Dedicated PSTN n/w Port mentioned above is configured as a network port on the RLC Port Configuration property sheet. ■ Ensure that the appropriate PBX Data port is configured and enabled.

Symptom**What to do**

The connection does not transfer from the IP network to the PSTN when the IP connection is lost.
(continued)

- 3 Ensure that "Type:Remote" or "Type:Local & Remote" and "Status:Enable" are selected for each active BRI channel (refer to "Configuring BRI Trunks" in the Remote Office 9150 Installation and Administration Guide NTP 555-8421-215).
- 4 Ensure that you selected "Status:Enable" in the Quality of Service window of the Remote Connection Configuration property sheet (refer to "Remote Connection Configuration" on page 171). Verify that the Signal Degrade slide in the same window is set to an acceptable level (refer to "Configuring Quality of Service" on page 182).
- 5 Understand that the QoS monitoring process monitors the network through sampling, according to the QoS Threshold slider settings. For testing purposes only, set the sliders to the far right and select one second in the Duration:Signal Degrade field.

Using Configuration Manager PING

PING, or Packet InterNet Groper, is a protocol and program to test whether a device is accessible on a network. This section explains how to use the PING option provided in Configuration Manager to verify connectivity. Use this procedure as a troubleshooting tool to determine if you can reach the remote unit, another RLC, or any other device on the network.

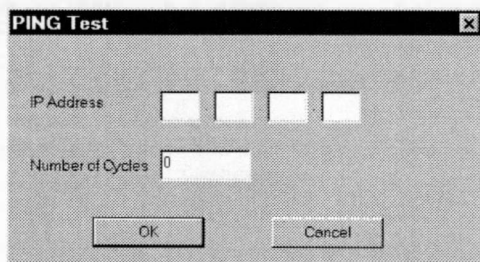
Getting there RLC → Configuration Manager

Performing a Configuration Manager PING

To perform a Configuration Manager PING:

- 1 From the Menu Bar, choose Tests → Ping.

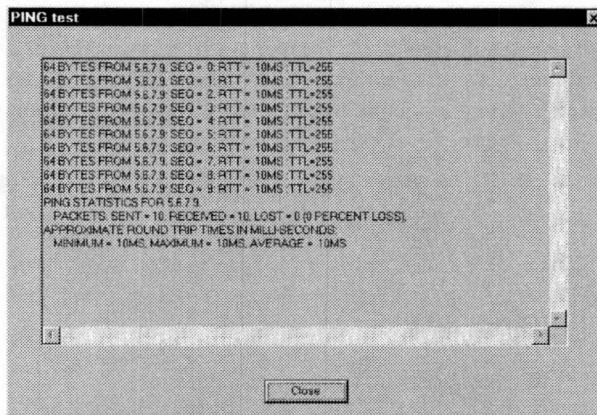
Result: The PING Test dialog box displays, similar to the following:



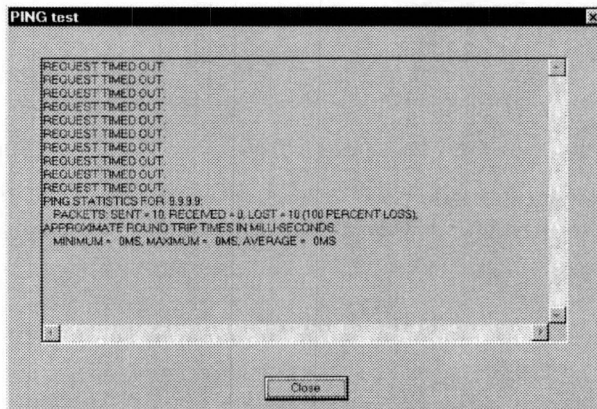
- 2 Enter the IP Address of the unit you want to PING in the IP Address field.
- 3 Enter the number of times you want to PING the unit in the Number of Cycles field (1 to 100).

- Click on the **OK** button.

Result: The PING test window displays, showing the PING results. The following is an example of a successful PING.



The following is an example of an unsuccessful PING.



- Click on the **Close** button.

Result: The PING test window closes.

ATTENTION

It is possible to successfully PING a device on the network and still not be able to log on to that device. If you log on to a device (an RLC) using a serial connection and neglect to log off, you may be able to successfully PING the device but be unable to establish a Telnet connection to it. (The device believes itself to be busy.)

If you cannot log on to a device after a successful PING, access the serial port and ensure that you are not logged on to the device through this port.

Unsuccessful PING options

If the PING was unsuccessful, answer these questions:

- 1** Did you enter the IP address correctly?
- 2** Are the subnet mask and default gateway configured properly at your site? (Confirm this by checking the IP Configuration property sheets for the involved units.)
- 3** Are the subnet mask and default gateway configured properly at the site that you are PINGing? (Confirm with the site's network administrator.)
- 4** Does the gateway respond to a PING?

If you are able to answer "Yes" to the questions above and the PING still does not work, the problem lies somewhere in the network between the involved sites.

Responding to a catastrophic failure

For the purposes of this discussion, a *catastrophic failure* is defined as a failure of the equipment to operate after review of all troubleshooting information and implementation of appropriate procedures.

Inoperative hardware

Should your RLC fail to operate after thorough review of the troubleshooting information in this and related Guides, consult your Nortel Networks distributor for hardware replacement.

Repair and warranty information

The RLC contains no user-serviceable components. If the problem experienced with your RLC persists after you have used all the appropriate procedures in this chapter, refer to the following contact information for repair and warranty help, depending upon your location.

Note: If the RLC is causing harm to the telephone network, the telephone company may request that you disconnect it pending resolution of the problem.

Canada

Nortel Networks Service Selection Center
30 Norelco Drive
Weston, ON
Canada
M9L 2X6

Telephone: 1-888-977-9444

United States

Nortel Networks
Product Service Center
640 Massman Drive
Nashville, TN 37210
USA

Telephone: 1-800-251-1758

Europe

Nortel Networks (NI) Ltd.
FAO: Irish Express Cargo (IEC)
Raheen Industrial Estate
Raheen, Limerick
Ireland

Telephone: +33 4 9296 1568
Fax: +33 4 9296 1598

Asia/Pacific

Nortel Distribution Center
c/o ACCO Transport
21 South St. Unit#2
Rydalmere, NSW
2116 Australia

CALA

Note: When you need warranty and repair service in Central American and Latin American countries, you must first get an RR (repair and return) number from your Nortel Networks distributor before shipping to the Nortel CALA Repair Center.

Nortel c/o Wesbell
4019 S.W. 30th Avenue
Fort Lauderdale, FL 33312
USA
Notify: Receiving Department
RR no.:

Telephone:
Normal Service Hours (Monday through Friday, 8:00 a.m. to 5:00 p.m. Central Time): 1-954-851-8841
After Normal Hours (weekends and holidays): 1-888-594-8474

Fax: 1-954-581-2334

Appendix A

Planning forms

In this appendix

Completing the forms	276
Connection Information—16 ports	278
Connection Information—32 ports	283
Online/Offline Table Configuration	292
System expansion worksheet	293

Completing the forms

ATTENTION

Before you can assign RLC ports to remote users, you must determine the total remote user requirements for the RLC.

- 1 Assign users on the remote units to remote ports on the RLC.

Note: To do this effectively, obtain information from the configuration information forms for all remote units connected to this RLC.

Record the RLC port assignments in the "Port configuration" section on one of the following RLC forms (according to the type of RLC installed):

- Connection Information—16 ports
- Connection Information—32 ports

Users who are using an MCA to transmit data must be assigned to a PBX data port. Users who are using ATAs can be assigned to PBX voice or data ports. Configure ATA users as voice ports only if there are not enough free data ports. Refer to "Remote port configuration" on page 107 for more information.

Note: The Connection Information forms identify the maximum number of ports that can be associated with MCAs and ATAs that are used to transmit data.

- 2 If you want to route calls over the PSTN, designate RLC ports to be used as network ports. At the same time, identify the telephone number that will be used to establish the connection with the remote unit.

Note: You must assign Network ports to PBX data ports.

Record the network port assignments and remote unit PSTN numbers on the Connection Information form for your RLC type.

- 3 Record the IP address for each remote unit on the Connection Information form for your RLC type.
- 4 If the chosen security level is provisioned security, record the security identifier that each remote unit uses to validate connection requests.

Note: You must configure the same security level on both the RLC and remote unit.

- 5 On the same form, record the following items for the RLC in the "Reach Line Card information" section:
 - IP address, subnet mask, and gateway
 - security level, and if required, security identifier
- 6 If necessary, complete an RLC Online/Offline Table Configuration form for each remote unit.

Reach Line Card

Connection Information—16 ports

Complete one copy of this form for each line card.

Page 1 of 5

RLC information

IPE position: Loop: _____ Shelf: _____ Card: _____

IP address:

--	--	--	--

.

--	--	--	--

.

--	--	--	--

.

--	--	--	--

Subnet mask:

--	--	--	--

.

--	--	--	--

.

--	--	--	--

.

--	--	--	--

Default gateway:

--	--	--	--

.

--	--	--	--

.

--	--	--	--

.

--	--	--	--

Host PBX's ELAN IP address:

--	--	--	--

.

--	--	--	--

.

--	--	--	--

.

--	--	--	--

Host PBX's ELAN subnet mask:

--	--	--	--

.

--	--	--	--

.

--	--	--	--

.

--	--	--	--

Security level: ☐ No security is required ☐ Caller ID ☐ Provisioned Security*

*If the security level is *provisioned security*, RLC's security identifier:

Inbound _____

Outbound _____

Notes:

- This RLC provides 32 total ports. Ports 0–15 are Voice ports and ports 16–31 are Data ports. On the host PBX, you must configure Network ports or Remote ports that use MCAs or ATAs (for data transmission) as Data ports. If there are not enough free Data ports, you can configure Remote ports that use ATAs as Voice ports. You can configure Remote ports used for FAX support as either Voice ports or Data ports. Refer to documentation for your PBX for necessary procedures.
- QoS Transition Technology requires one MCA per B-channel.
- If you want to use MCAs or ATAs to transmit data, you can connect a maximum of four MCAs or ATAs to Remote ports on this RLC.

Reach Line Card

Connection Information—16 ports

Port configuration

Page 2 of 5

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address	Security ID (if Network port)
0	☐ Network ☐ Remote ☐ Local TCM	☐ Yes ☐ No			
1	☐ Network ☐ Remote ☐ Local TCM	☐ Yes ☐ No			
2	☐ Network ☐ Remote ☐ Local TCM	☐ Yes ☐ No			
3	☐ Network ☐ Remote ☐ Local TCM	☐ Yes ☐ No			
4	☐ Network ☐ Remote ☐ Local TCM	☐ Yes ☐ No			
5	☐ Network ☐ Remote ☐ Local TCM	☐ Yes ☐ No			
6	☐ Network ☐ Remote ☐ Local TCM	☐ Yes ☐ No			
7	☐ Network ☐ Remote ☐ Local TCM	☐ Yes ☐ No			
8	☐ Network ☐ Remote ☐ Local TCM	☐ Yes ☐ No			

Reach Line Card

Connection Information—16 ports

Port configuration (continued)

Page 3 of 5

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address	Security ID (if Network port)
9	☐ Network ☐ Remote ☐ Local TCM	☐ Yes ☐ No			
10	☐ Network ☐ Remote ☐ Local TCM	☐ Yes ☐ No			
11	☐ Network ☐ Remote ☐ Local TCM	☐ Yes ☐ No			
12	☐ Network ☐ Remote ☐ Local TCM	☐ Yes ☐ No			
13	☐ Network ☐ Remote ☐ Local TCM	☐ Yes ☐ No			
14	☐ Network ☐ Remote ☐ Local TCM	☐ Yes ☐ No			
15	☐ Network ☐ Remote ☐ Local TCM	☐ Yes ☐ No			
16	☐ Network ☐ Remote ☐ Local TCM	☐ Yes ☐ No			
17	☐ Network ☐ Remote ☐ Local TCM	☐ Yes ☐ No			

Reach Line Card**Connection Information—16 ports**

Port configuration (continued)

Page 4 of 5

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address	Security ID (if Network port)
18	☐ Network ☐ Remote ☐ Local TCM	☐ Yes ☐ No			
19	☐ Network ☐ Remote ☐ Local TCM	☐ Yes ☐ No			
20	☐ Network ☐ Remote ☐ Local TCM	☐ Yes ☐ No			
21	☐ Network ☐ Remote ☐ Local TCM	☐ Yes ☐ No			
22	☐ Network ☐ Remote ☐ Local TCM	☐ Yes ☐ No			
23	☐ Network ☐ Remote ☐ Local TCM	☐ Yes ☐ No			
24	☐ Network ☐ Remote ☐ Local TCM	☐ Yes ☐ No			
25	☐ Network ☐ Remote ☐ Local TCM	☐ Yes ☐ No			
26	☐ Network ☐ Remote ☐ Local TCM	☐ Yes ☐ No			

Reach Line Card

Connection Information—16 ports

Port configuration (continued)

Page 5 of 5

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address	Security ID (if Network port)
27	☐ Network ☐ Remote ☐ Local TCM	☐ Yes ☐ No			
28	☐ Network ☐ Remote ☐ Local TCM	☐ Yes ☐ No			
29	☐ Network ☐ Remote ☐ Local TCM	☐ Yes ☐ No			
30	☐ Network ☐ Remote ☐ Local TCM	☐ Yes ☐ No			
31	☐ Network ☐ Remote ☐ Local TCM	☐ Yes ☐ No			

Reach Line Card

Connection Information—32 ports

Port configuration

Page 2 of 9

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address	Security ID (if Network port)
Slot 1					
0	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
1	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
2	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
3	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
4	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
5	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
6	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
7	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
8	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			

Reach Line Card

Connection Information—32 ports

Port configuration (continued)

Page 3 of 9

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address	Security ID (if Network port)
9	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
10	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
11	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
12	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
13	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
14	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
15	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
16	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
17	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			

Reach Line Card

Connection Information—32 ports

Port configuration (continued)

Page 4 of 9

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address	Security ID (if Network port)
18	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
19	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
20	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
21	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
22	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
23	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
24	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
25	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
26	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			

Reach Line Card

Connection Information—32 ports

Port configuration (continued)

Page 5 of 9

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address	Security ID (if Network port)
27	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
28	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
29	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
30	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
31	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			

Reach Line Card

Connection Information—32 ports

Port configuration (continued)

Page 6 of 9

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address	Security ID (if Network port)
Slot 2					
32	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
33	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
34	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
35	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
36	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
37	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
38	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
39	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
40	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			

Reach Line Card

Connection Information—32 ports

Port configuration (continued)

Page 7 of 9

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address	Security ID (if Network port)
41	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
42	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
43	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
44	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
45	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
46	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
47	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
48	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
49	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			

Reach Line Card

Connection Information—32 ports

Port configuration (continued)

Page 8 of 9

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address	Security ID (if Network port)
50	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
51	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
52	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
53	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
54	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
55	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
56	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
57	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
58	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			

Reach Line Card

Connection Information—32 ports

Port configuration (continued)

Page 9 of 9

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address	Security ID (if Network port)
59	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
60	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
61	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
62	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			
63	☐ Network ☐ Remote ☐ Local telephone	☐ Yes ☐ No			

Reach Line Card

Online/Offline Table Configuration

Page 1 of 1

 RLC unit number: _____ 254 _____ Remote unit number: _____
Notes:

- If a schedule is not defined for this remote site, the digital telephone online/offline status is defined solely by the remote site user dialing the online/offline SPRE code on the telephone.
- The schedule, if configured, does not prevent this site from establishing or terminating a connection to the network. Schedule entries can be overridden by the site user by dialing the online/offline SPRE code on the telephone.

Day	On	Off	On	Off	On	Off	On	Off
Monday	_____	_____	_____	_____	_____	_____	_____	_____
	_____	_____	_____	_____	_____	_____	_____	_____
Tuesday	_____	_____	_____	_____	_____	_____	_____	_____
	_____	_____	_____	_____	_____	_____	_____	_____
Wednesday	_____	_____	_____	_____	_____	_____	_____	_____
	_____	_____	_____	_____	_____	_____	_____	_____
Thursday	_____	_____	_____	_____	_____	_____	_____	_____
	_____	_____	_____	_____	_____	_____	_____	_____
Friday	_____	_____	_____	_____	_____	_____	_____	_____
	_____	_____	_____	_____	_____	_____	_____	_____
Saturday	_____	_____	_____	_____	_____	_____	_____	_____
	_____	_____	_____	_____	_____	_____	_____	_____
Sunday	_____	_____	_____	_____	_____	_____	_____	_____
	_____	_____	_____	_____	_____	_____	_____	_____

Reach Line Card System expansion worksheet

Page 1 of 4

Number of DSP application modules needed

Complete one worksheet for each RLC.

- 1 How many remote users do you want to support?

Notes:

- Up to 16 users can be connected to the NTDR68xx Line Card. Up to 32 users can be connected to the NTDR70xx or NTDR71xx Line Cards.
- If using ATAs or MCAs to transmit data, the NTDR68xx Line Card supports up to four ATAs or MCAs. NTDR70xx or NTDR71xx Line Cards support up to seven ATAs or MCAs. Each ATA requires the resources of one DSP channel for data transmission.

- 2 Do you want to implement call blocking? (Users will receive a fast busy signal when resources are not available.) ☐ Yes ☐ No

- 3 If step 2 is Yes, calculate the number of calls that can be active at one time.

Note: A conservative estimate of one call in three being blocked when no resources are available is recommended.

Multiply your step 1 answer by your call blocking factor. For example, to calculate the number of simultaneous calls that can be supported at a 3 to 2 blocking ratio, multiply your step 1 answer by 2/3 (0.666). If the result contains a fraction, round up to a whole number.

Step 1: _____ x _____ = _____

If step 2 is No, the number of simultaneous calls is the same as the number of user stations installed. (Record your response to line 1 here.) _____

Reach Line Card

System expansion worksheet

Page 2 of 4

Number of DSP application modules needed (continued)

- 4 Divide your step 3 answer by 8, then round down the result to a whole number.

Step 3: _____ / 8 = _____

The total number of DSP channels required at the local site equals the total number of simultaneous remote service telephone calls you want to allow on your entire remote network. This includes calls from Remote Office 9150, 9110, 9115 units, and Meridian Digital Telephone IP Adapter units (Internal and External). Assuming that there are eight voice channels available on a single DSP application module (the current DSP application module channel capacity), and taking into account the eight built-in DSP channels on the RLC and Remote Office 9150 mother boards, determine the number of DSP application modules required on your host PBX using the following equations:

A: voice DSP devices required =
simultaneous remote service voice channels for 9150 and 911x / 4

B: 911x DSP devices required =
simultaneous PSTN connections for 911x / 4

total DSP devices required = A + B - 2

Note: Each DSP application module consists of two DSP devices.

Reach Line Card

System expansion worksheet

Page 3 of 4

Number of DSP application modules needed (continued)

(step 4 continued) If the result of equations A or B is a fraction, round *up* to the nearest whole number. For example, for simultaneous 17 remote service telephone calls and zero PSTN connections for 911x, the equations are as follows:

$$\text{A: voice DSP devices required} = 17 / 4 = 4.25 = 5$$

(For 17 remote service calls, the equation works out to 4.25 and rounds up to five.)

$$\text{B: 911x DSP devices required} = 0 / 4 = 0$$

$$\text{total DSP required} = 5 + 0 - 2 = 3$$

$$\text{total DSP application modules required} = 2$$

A remote network supporting 17 simultaneous remote service telephone calls requires two DSP application modules.

If the RLC supports more than one remote site, remember that its DSP application modules must support the voice processing for all sites combined.

- 5 Record the number of DSP application modules already installed.
Note: The RLC shipped from Nortel Networks with one DSP module built in.
 Your response here must include that module.

- 6 Calculate how many DSP modules you need to purchase.
 Subtract your step 8 answer from your step 4 answer.
Note: Only four DSP application modules can be installed on the NTDR68xx Line Card. Up to four DSP application modules can be installed on the NTDR70xx or NTDR71xx Line Cards.

- 7 Allow for future growth?

☐ Yes

☐ No

Note: All users at a Remote Office 9150 site must be assigned to one RLC only. Therefore, future assignment of RLC ports should be considered.

For example, if a Remote Office 9150 site grows from 8 to 20 users, and 12 more ports are not available on the RLC, then you must reassign of the entire Remote Office 9150 site (20 users) to another RLC.

Reach Line Card

System expansion worksheet

Page 4 of 4

Number of DSP application modules needed (continued)

- 8 Record the number of DSP application modules already installed.

Note: The RLC shipped from Nortel Networks with one DSP module built in. Your response here must include that module.

- 9 Calculate how many DSP modules you need to purchase.

Subtract your step 8 answer from your step 4 answer.

Note: Only four DSP application modules can be installed on the NTDR68xx Line Card. Up to four DSP application modules can be installed on the NTDR70xx or NTDR71xx Line Cards.

- 10 Allow for future growth?

☐ Yes☐ No

Note: All users at a Remote Office 9150 site must be assigned to one RLC only. Therefore, future assignment of RLC ports should be considered.

For example, if a Remote Office 9150 site grows from 8 to 20 users, and 12 more ports are not available on the RLC, then you must reassign of the entire Remote Office 9150 site (20 users) to another RLC.

Appendix B

Sample configuration files

In this appendix

Example of a network	300
Voice port configuration on the Meridian 1 PBX	302
Data port configuration for 9150 on the Meridian 1 PBX	304
Data port configuration for 911x on the Meridian 1 PBX	306
Voice port configuration on the MSL-100 PBX	308
Data port configuration for 9150 on the MSL-100 PBX	310
Data port configuration for 911x on the MSL-100 PBX	313
RLC configuration	315
Remote Office 9150 unit configuration	319
Remote Office 911x series unit configuration	322

Example of a network

This section provides an example of a network diagram that shows one host site (with one RLC installed on the host PBX) and one Remote Office 9150 unit (with one user station). The purpose of this diagram is to demonstrate the relationship between configuration settings on each unit in the network.

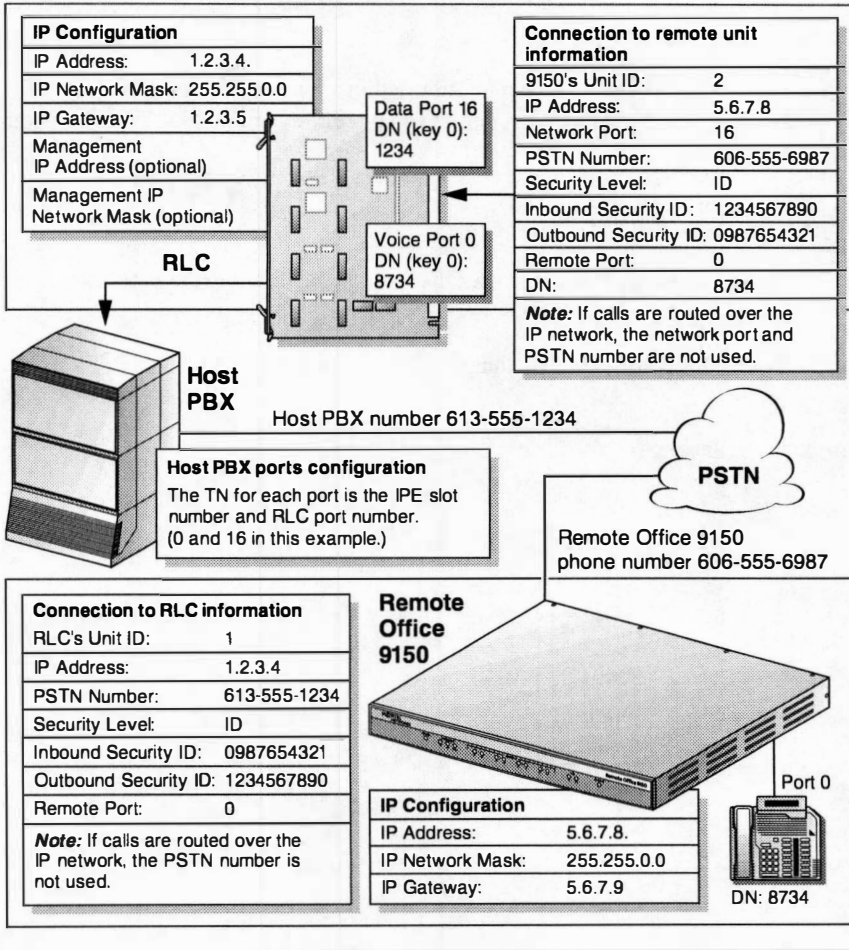
Configuration recommendation

The quickest way to configure the RLC, Remote Office 9150 unit, and Remote Office 911x series unit is to run the Configuration Wizard. For instructions, refer to “Using the Configuration Wizard to perform initial configuration” on page 83. For your reference, the Configuration Wizard screen examples are completed using the same information.

Note: The network diagram shows information that cannot be configured through the Configuration Wizard, such as the security identifiers. You must use Configuration Manager to complete the configuration.

Network diagram

Note: This diagram assumes that both the IP and PSTN are being used.



G101413

Voice port configuration on the Meridian 1 PBX

This section shows the configuration settings for the voice port on the Meridian 1 PBX. Generally, define voice ports according to the needs of your remote users.

Configuration example

This configuration example uses the settings identified in the network diagram shown on page 301.

Note: This configuration example is from a Meridian 1 Option 11.

```
REQ: prt
TYPE: 2616
MARF NOT ACTIVATED
```

Telephone type

```
TN 5 0
DATE
PAGE
DES
```

```
DES Bryan Dion
TN 005 0 00 00
```

RLC slot and port numbers

```
TYPE 2616
CDEN 8D
CUST 0
AOM 0
FDN
TGAR 1
LDN NO
NCOS 0
SGRP 0
RNPG 0
SCI 0
SSU
XLST
```

```

CLS   CTD FBD WTA LPR MTD FND HTD ADD HFD
      MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
      POD DSX VMD CMSD CCSD SWD LND CNDD
      CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBF
      ICDD CDMD LLCN MCTD CLBD AUTU
      GPUD DPUD DNDD CFXD ARHD CLTD ASCD
      CPFA CPTA ABDD CFHD FICD NAID BUZZ AHD
      DDGA NAMA
      DRDD EXR0
      USMD USRD ULAD RTDD RBDD RBHD PGND FLXD FTTC DNDY DNO3
CPND_LANG ENG
HUNT
PLEV 02
AST
IAPG 0
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
DNDR 0
KEY 00 SCR 8734 0      MARP
      CPND
      NAME Bryan Dion
      XPLN 24
      DISPLAY_FMT FIRST, LAST
01 CWT
02 MSB
03 TRN
04 CFW 4
05 AO6
06
07
08
09
10 MCR 8234 0 MARP
      CPND
      NAME Bryan Dion
      XPLN 24
      DISPLAY_FMT FIRST, LAST
11 AO6
12
13 DSP
14
15

```

VCE defines the port as a voice port.

User's DN

User's CPND

Data port configuration for 9150 on the Meridian 1 PBX

This section shows the configuration settings for the data port on the Meridian 1 PBX. The data port provides the communication path between the RLC and the Remote Office 9150 unit, and must be configured as an MCA.

Configuration example

This configuration example uses the settings identified in the network diagram shown on page 301.

Note: This configuration sample is from a Meridian 1 Option 11.

```

REQ: prt
TYPE: 2616
TN 5 16
DES
DES Remote site 1
TN 005 0 00 16
TYPE 2616
CDEN 8D
CUST 0
AOM 0
FDN
TGAR 1
LDN NO
NCOS 0
SGRP 0
RNPG 0
SCI 0
SSU
XLST
CLS CTD FBD WTD LPR MTD FND HTD ADD HFD
MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD DTA DRG1
POD DSX VMD CMSD CCSD SWD LND CNDD
CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBF
ICDD CDMD LLCN MCTD CLBD AUTU
GPUD DPUD DNDD CFXD ARHD CLTD ASCD
CPFA CPTA ABDD CFHD FICD NAID BUZZ AHD
DDGA NAMA
DRDD EXR0
USMD USRD ULAD RTDD RBDD RBHD PGND FLXD FTTC DNDY DNO3

```

← Telephone type

← RLC slot and port numbers

TGAR must be configured to allow trunk access. Refer to your PBX documentation for more details.

DTA defines the port as a data port.


```
TOV 0 MINS
DTAO MCA
PSEL DMDM
HUNT
PSDS NO
TRAN ASYN
PAR SPACE
DTR ON
DUP FULL
HOT OFF
AUT ON
BAUD 56000
DCD ON
PRM KBD ON
VLL OFF
MOD YES
INT OFF
CLK OFF
KBD ON
RTS OFF
PLEV 02
AST
IAPG 0
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
DNDR 0
KEY 00 SCR 1234 0 MARP
    01
    02
    03
    04
    05
    06
    07
    08
    09
    10
    11
    12
    13
    14
    15
```

Network ports must be defined as MCA.

Baud defaults to 56K, however, the RLC determines actual Baud on a per-call basis.

The number that the Remote Office 9150 unit needs to connect to the RLC. It must be a DID number.

Data port configuration for 911x on the Meridian 1 PBX

This section shows the configuration settings for the data port on the Meridian 1 PBX. The data port provides the communication path between the RLC and the Remote Office 911x series unit, and must be configured as an ATA.

Configuration example

This configuration sample is from a Meridian 1 Option 11.

```
REQ: prt
TYPE: 2616
MARP NOT ACTIVATED
TN 9 16
DATE
PAGE
DES
DES NO DES
TN 009 0 00 16
TYPE 2616
CDEN 8D
CUST 0
AOM 0
FDN
TGAR 1
LDN NO
NCOS 0
SGRP 0
RNPG 0
SCI 0
SSU
XLST
SFLT NO
CAC_CIS 3
CAC_MFC 0
```

← Telephone type

← RLC slot and port numbers

← TGAR must be configured to allow trunk access. Refer to your PBX documentation for more details.

VCE defines the port as a voice port.

CLS CTD FBD WTA LPR MTD FND HTD ADD HFD
 MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
 POD DSX VMD CMSD SLKD CCSD SWD LND CNDD
 CFTD SFD MRD DDV CNIA CDCA MSID DAPA BFED RCBF
 ICDD CDMD LLCN MCTD CLBD AUTU
 GPUD DPUD DNDD CFXD ARHD CLTD ASCD
 CPFA CPTA HSPD ABDD DELD CFHD FICD NAID DNAA BUZZ AGRD MOAD
 UDI RCC HBTD AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
 DRDD EXR0
 USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBF FLXA FTTC DNDY DNO
 MCBN
 CPND_LANG ENG
 HUNT
 PLEV 02
 AST
 IAPG 0
 AACN NO
 ITNA NO
 DGRP
 MLWU_LANG 0
 DNDR 0
 DTMK
 KEY 00 SCR 9016 0 MARP
 ANIE 0
 01
 02
 03
 04
 05
 06
 07
 08
 09
 10
 11
 12
 13
 14
 15

The number that the Remote Office 911x series unit needs to connect to the RLC. It must be a DID number.

Voice port configuration on the MSL-100 PBX

This section shows the datafill for a typical M2616 subscriber line. Voice ports (telephones) must be datafilled on the even numbered LENs in the SL-100. The even numbered ports correspond to ports 0-15 on both the RLC at the host site, and the Remote Office 9110, 9115, or 9150 unit(s) at the remote site(s) served by the RLC.

Configuration example

```
>table lninv
TABLE: LNINV
>add
LEN:
>host 19 1 4 0          ← This is the LEN address in the Meridian SL100
CARDCODE:
>DR68AA                 ← This is the card that will be occupying the IPE slot
PADGRP:
>DONS
STATUS:
>hasu                   ← HASU , meaning Hardware Assigned, Software
Unassigned
GND:
>n
BNV:
>nl
MNO:
>y
CARDTYPE:
>nil
TUPLE TO BE ADDED:
HOST 19 1 04 0 DR68AA DONS HASU N NL Y      NIL
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y

>servord
SO:
>new
```

This is an example of a typical M2616 telephone set:

```

SONUMBER:      NOW    0   9  22 PM
>
DN:
>6846100      ← Site Specific information, is the DN of the instrument
LCC_ACC:
>m2616        ← Telephone Type.
RINGTYPE:
>fh
HANDS_FREE:
>y
GROUP:
>ntirich      ← Site Specific information. This will vary between sites
SUBGRP:
>0            ← Site Specific information. This will vary between sites
NCOS:
>64           ← Site Specific information. This will vary between sites
SNPA:
>972          ← Site Specific information. This will vary between sites
KEY:
>1
RINGING:
>y
LEN_OR_LTID:
>19 1 4 0     ← This is the LEN of the Voice Port.
OPTKEY:
>1
OPTION:
>m0200        ← This is the option for a display.
OPTKEY:
>$
COMMAND AS ENTERED:
NEW NOW 0 9 22 PM 9726100 M2616 FH Y NTIRICH 0 64 972 1 Y HOST 19 1 04
00 ( 1
M0200 ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
2000/09/22 12:34:41.571 FRI.    JOURNAL FILE RECORD ID 62

```

Data port configuration for 9150 on the MSL-100 PBX

This section shows the configuration settings for the MCA data port on the MSL-100 PBX. The data port provides the communication path between the RLC and the Remote Office 9150 unit, and must be configured as an MCA. MCAs must be datafilled on the odd numbered LENS in the MSL-100. The odd numbered ports correspond to ports 16-32 on both the RLC and the Remote Office 9150 unit.

Configuration example

```
>table lninv
TABLE: LNINV
>add
LEN:
>host 19 1 4 31          ← This is the LEN address in the Meridian MSL-100.
CARDCODE:
>DR68AA                 ← This is the card that will be occupying the IPE slot.
PADGRP:
>DONS
STATUS:
>hasu                   ← HASU , meaning Hardware Assigned, Software
Unassigned
GND:
>n
BNV:
>n1
MNO:
>y
CARDTYPE:
>n11
TUPLE TO BE ADDED:
HOST 19 1 04 31   DR68AA   DONS   HASU   N   NL   Y   NIL
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y

>servord
SO:
>new
SONUMBER:      NOW      0   9 21 AM
```

MSL-100 Data port configuration (cont'd.)

DN:	
>6846789	← Site Specific information. This will vary between sites.
LCC_ACC:	
>mca	← Field denotes line type.
GROUP:	
>NTIRICH	← Site Specific information. This will vary between sites.
SUBGRP:	
>0	← Site Specific information. This will vary between sites.
NCOS:	
>64	← Site Specific information. This will vary between sites.
SNPA:	
>972	← Site Specific information. This will vary between sites.
RINGING:	
>y	
CLASSDU:	
>mca	
DOWNLOAD:	
>n	
SYNCHRO:	
>s	
DATARATE:	
>64000	
CLOCKSRC:	
>i	
V25:	
>n	
HDLC:	
>n	
RTS:	
>n	
HOTLINE:	
>n	
VLL:	
>n	
IDLETO:	
>0	
KBDTYP:	
>hayes	
DPOPTS:	
>\$	
LATANAME:	
>nillata	

MSL-100 Data port configuration (cont'd.)

```
LEN_OR_LTID:
>19 1 4 31
OPTION:
>ndc
OPTION:
>$
COMMAND AS ENTERED:
NEW NOW 0 9 21 AM 6846789 MCA NTIRICH 0 64 972 Y MCA N S 64000 I N N N
N N
0 HAYES $ NILLATA HOST 19 1 04 31 ( NDC ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
```

← Site Specific information. This will vary between sites.

Data port configuration for 911x on the MSL-100 PBX

This section shows the configuration settings for the ATA data port on the MSL-100 PBX. The data port provides the communication path between the RLC and the Remote Office 911x unit, and must be configured as an ATA. ATAs must be datafilled on the odd numbered LENS in the MSL-100. The odd numbered ports correspond to ports 16-32 on both the RLC and the Remote Office 911x series unit.

Configuration example

```
TABLE: LNINV
>pos 19 1 06 03
HOST 19 1 06 03   DR68AA   DONS   WORKING   N   NL   Y
FLXA
>cha
CARDCODE: DR68AA
>
PADGRP: DONS
>
STATUS: WORKING
>
GND: N
>BNV: NL
>MNO: Y
>CARDTYPE: FLXA  ← Must be FLXA for 911x network port.
>
TUPLE TO BE CHANGED:
HOST 19 1 06 03   DR68AA   DONS   WORKING   N   NL   Y
FLXA
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
LEN:      HOST 19 1 06 03 ← This is the LEN address in the Meridian MSL-100.
TYPE: SINGLE PARTY LINE
SNPA: 972
DIRECTORY NUMBER:      6846779
LINE CLASS CODE:  M3904 WITH HANDSFREE
```

This is the card that will be occupying the IPE slot.

↓

CUSTGRP: NTIRICH SUBGRP: 0 NCOS: 64 RING: Y
CARDCODE: DR68AA GND: N PADGRP: DONS BNV: NL MNO: Y
PM NODE NUMBER : 163
PM TERMINAL NUMBER : 196
DNGRPS OPTIONS:
NETNAME: NORTEL
ADDRESS: DDD44NNNNN
NETNAME: PUBLIC
ADDRESS: 97268NNNNN
OPTIONS:
NONE

KEY	DN
---	--
1	DN 9726846779

KEY	FEATURE
---	-----
NONE	

RLC configuration

This section shows the configuration settings for the RLC. You can obtain a similar configuration printout by performing a configuration download while connected to the RLC.

Note: Configuration settings are separated by commas (,).

Configuration example

This configuration example uses the settings identified in the network diagram shown on page 301.

SYSCFG 254,HOST1

APPMODCFG 0,NC,NC
 APPMODCFG 1,E,G729,G729
 APPMODCFG 2,NC,NC
 APPMODCFG 3,NC,NC

RLC's IP address information:

- Unit ID
- Site Name

SYSCFG 254,HOST1

RLCCFG E,E
 ACCFG D

DSP application module
 (only module 1 is configured
 in this case)

Unit ID and node name

PORTCFG 0,1,0,2,2,D
 PORTCFG 1,1,0,2,2,D
 PORTCFG 2,1,0,2,2,D
 PORTCFG 3,1,0,2,2,D
 PORTCFG 4,1,0,2,2,D
 PORTCFG 5,1,0,2,2,D

Ports configured as remote ports

```

PORTCFG 6,0
PORTCFG 7,0
PORTCFG 8,0
PORTCFG 9,0
PORTCFG 10,0
PORTCFG 11,0
PORTCFG 12,0
PORTCFG 13,0
PORTCFG 14,0
PORTCFG 15,0

```

Ports configured
as local ports



```

PORTCFG 16,2,2,6065556987

```

```

PORTCFG 17,0
PORTCFG 18,0
PORTCFG 19,0
PORTCFG 20,0
PORTCFG 21,0
PORTCFG 22,0
PORTCFG 23,0
PORTCFG 24,0
PORTCFG 25,0
PORTCFG 26,0
PORTCFG 27,0

```

Port configured
as network port



```

.
.
.
PORTCFG 63,0

```

```

RUNITCFG 1,E,0,2,45,45,3,1234567890,0987654321,E,Y,5.6.7.8,
E,16,D,16,10,Y,6065556987,D

```

```

RUNITCFG 2,D,0,0,2,1,1,D,D,D
RUNITCFG 3,D,0,0,2,1,1,D,D,D
RUNITCFG 4,D,0,0,2,1,1,D,D,D
RUNITCFG 5,D,0,0,2,1,1,D,D,D
RUNITCFG 6,D,0,0,2,1,1,D,D,D
RUNITCFG 7,D,0,0,2,1,1,D,D,D
RUNITCFG 8,D,0,0,2,1,1,D,D,D
RUNITCFG 9,D,0,0,2,1,1,D,D,D
RUNITCFG 10,D,0,0,2,1,1,D,D,D

```

Remote unit connection
information (unit 1):



- remote unit number
- unit ID
- security information (inbound and outbound security IDs)
- remote unit's IP address
- network port
- PSTN number

```
ONOFFCFG 1,SUN,0 00:00
ONOFFCFG 1,MON,0 00:00
ONOFFCFG 1,TUE,0 00:00
ONOFFCFG 1,WED,0 00:00
ONOFFCFG 1,THU,0 00:00
ONOFFCFG 1,FRI,0 00:00
ONOFFCFG 1,SAT,0 00:00
ONOFFCFG 2,SUN,0 00:00
ONOFFCFG 2,MON,0 00:00
ONOFFCFG 2,TUE,0 00:00
ONOFFCFG 2,WED,0 00:00
ONOFFCFG 2,THU,0 00:00
ONOFFCFG 2,FRI,0 00:00
ONOFFCFG 2,SAT,0 00:00
ONOFFCFG 3,SUN,0 00:00
ONOFFCFG 3,MON,0 00:00
ONOFFCFG 3,TUE,0 00:00
ONOFFCFG 3,WED,0 00:00
ONOFFCFG 3,THU,0 00:00
ONOFFCFG 3,FRI,0 00:00
ONOFFCFG 3,SAT,0 00:00
ONOFFCFG 4,SUN,0 00:00
ONOFFCFG 4,MON,0 00:00
ONOFFCFG 4,TUE,0 00:00
ONOFFCFG 4,WED,0 00:00
ONOFFCFG 4,THU,0 00:00
ONOFFCFG 4,FRI,0 00:00
ONOFFCFG 4,SAT,0 00:00
ONOFFCFG 5,SUN,0 00:00
ONOFFCFG 5,MON,0 00:00
ONOFFCFG 5,TUE,0 00:00
ONOFFCFG 5,WED,0 00:00
ONOFFCFG 5,THU,0 00:00
ONOFFCFG 5,FRI,0 00:00
ONOFFCFG 5,SAT,0 00:00
ONOFFCFG 6,SUN,0 00:00
ONOFFCFG 6,MON,0 00:00
ONOFFCFG 6,TUE,0 00:00
ONOFFCFG 6,WED,0 00:00
ONOFFCFG 6,THU,0 00:00
ONOFFCFG 6,FRI,0 00:00
```

← Online/offline schedule

```

ONOFFCFG 6,SAT,0 00:00
ONOFFCFG 7,SUN,0 00:00
ONOFFCFG 7,MON,0 00:00
ONOFFCFG 7,TUE,0 00:00
ONOFFCFG 7,WED,0 00:00
ONOFFCFG 7,THU,0 00:00
ONOFFCFG 7,FRI,0 00:00
ONOFFCFG 7,SAT,0 00:00
ONOFFCFG 8,SUN,0 00:00
ONOFFCFG 8,MON,0 00:00
ONOFFCFG 8,TUE,0 00:00
ONOFFCFG 8,WED,0 00:00
ONOFFCFG 8,THU,0 00:00
ONOFFCFG 8,FRI,0 00:00
ONOFFCFG 8,SAT,0 00:00
ONOFFCFG 9,SUN,0 00:00
ONOFFCFG 9,MON,0 00:00
ONOFFCFG 9,TUE,0 00:00
ONOFFCFG 9,WED,0 00:00
ONOFFCFG 9,THU,0 00:00
ONOFFCFG 9,FRI,0 00:00
ONOFFCFG 9,SAT,0 00:00
ONOFFCFG 10,SUN,0 00:00
ONOFFCFG 10,MON,0 00:00
ONOFFCFG 10,TUE,0 00:00
ONOFFCFG 10,WED,0 00:00
ONOFFCFG 10,THU,0 00:00
ONOFFCFG 10,FRI,0 00:00
ONOFFCFG 10,SAT,0 00:00

```

```

FBQOSCFG 1,E,5,6,5,10,10,32
FBQOSCFG 2,D,5,6,5,10,10,32
FBQOSCFG 3,D,5,6,5,10,10,32
FBQOSCFG 4,D,5,6,5,10,10,32
FBQOSCFG 5,D,5,6,5,10,10,32
FBQOSCFG 6,D,5,6,5,10,10,32
FBQOSCFG 7,D,5,6,5,10,10,32
FBQOSCFG 8,D,5,6,5,10,10,32
FBQOSCFG 9,D,5,6,5,10,10,32
FBQOSCFG 10,D,5,6,5,10,10,32

```

Item not Configured

Quality of Service settings
(these are default settings)

Caller ID (not configured;
one line for each remote
unit)

Remote Office 9150 unit configuration

This section shows the configuration settings for the Remote Office 9150 unit. You can obtain a similar configuration printout by performing a configuration download while connected to the Remote Office 9150 unit.

Note: Configuration settings are separated by commas (,).

Configuration example

This configuration example uses the settings identified in the network diagram shown on page 301.

```

IPCFCF 5.6.7.8,255.255.0.0,5.6.7.9
APPMODCFG 0,SPARE,TSIDSP
APPMODCFG 1,E,G729,G729
APPMODCFG 2,NC,NC
APPMODCFG 3,NC,NC
APPMODCFG 4,1,1,E,1,1,5556987,60655569870101,E,1,1,
5556988,60655569880101
APPMODCFG 5,NC,NC
APPMODCFG 6,NC,NC
APPMODCFG 7,NC,NC
SYSCFG 2, Remote site 1
ROUCFG 13:00,0,JAN-13-2000,911,#222,#333,#345,#456,E
ACCFG N
  
```

9150 unit's IP interface information

- IP address
- Subnet mask
- IP gateway

On-board DSP module (module 0) and installed DSP application module (module 1)

ISDN BRI module configuration

- module number
- PSTN number for each B-channel
- SPID for each B-channel

Unit ID and node name

System configuration:

- Emergency service number
- System date and time
- SPRE codes

RLCDETCFG 254,3,0987654321,1234567890,E,1.2.3.4,E,6135551234,E,D

Host PBX connection
information:

- RLC's unit ID
- security information (inbound and outbound)

ROUDEVCFG 0,2,0,E,E,E,Bryan Dion,8734,04
 ROUDEVCFG 1,2,1,E,E,E,Marc Horman,8707,04
 ROUDEVCFG 2,2,2,E,E,E,Brad McAllister,8708,04
 ROUDEVCFG 3,2,3,E,E,E,Andrew Wong,8760,04
 ROUDEVCFG 4,2,4,E,E,E,Corey Smith,8709,04
 ROUDEVCFG 5,2,5,E,E,E,Tracey Black,8743,04
 ROUDEVCFG 6,0,E,E,E,John Brown,8611,04

Port (station) configuration:

- Port number
- Local and remote capability
- CPID

ROUDEVCFG 7,1,0
 ROUDEVCFG 8,1,0
 ROUDEVCFG 9,1,0
 ROUDEVCFG 10,1,0
 ROUDEVCFG 11,1,0
 ROUDEVCFG 12,1,0
 ROUDEVCFG 13,1,0
 ROUDEVCFG 14,1,0
 ROUDEVCFG 15,1,0
 ROUDEVCFG 16,1,0
 ROUDEVCFG 17,1,0
 ROUDEVCFG 18,1,0
 ROUDEVCFG 19,1,0
 ROUDEVCFG 20,1,0
 ROUDEVCFG 21,1,0
 ROUDEVCFG 22,1,0
 ROUDEVCFG 23,1,0
 ROUDEVCFG 24,1,0
 ROUDEVCFG 25,1,0
 ROUDEVCFG 26,1,0
 ROUDEVCFG 27,1,0
 ROUDEVCFG 28,1,0
 ROUDEVCFG 29,1,0
 ROUDEVCFG 30,1,0
 ROUDEVCFG 31,1,0
 ROUDEVCFG 64,2,31,E,E,E,FAX,8664,900

Unconfigured ports
Note: The default capability is Remote.

Fax port configuration:

- Port number
- Local and remote capability
- CPID


```

FKEYCFG 0,2 TRN 12345678,3 CFW 4000,8 LC1 ,9 LC2 ,NC
FKEYCFG 1,2 TRN 12345678,3 CFW 4000,8 LC1 ,9 LC2 ,NC
FKEYCFG 2,2 TRN 12345678,3 CFW 4000,8 LC1 ,9 LC2 ,NC
FKEYCFG 3,2 TRN 12345678,3 CFW 4000,8 LC1 ,9 LC2 ,NC
FKEYCFG 4,2 TRN 12345678,3 CFW 4000,8 LC1 ,9 LC2 ,NC
FKEYCFG 5,2 TRN 12345678,3 CFW 4000,8 LC1 ,9 LC2 ,NC
FKEYCFG 6,8 LC1 ,9 LC2 ,NC
FKEYCFG 7,NC
FKEYCFG 8,NC
FKEYCFG 9,NC
FKEYCFG 10,NC
FKEYCFG 11,NC
FKEYCFG 12,NC
FKEYCFG 13,NC
FKEYCFG 14,NC
FKEYCFG 15,NC
FKEYCFG 16,NC
FKEYCFG 17,NC
FKEYCFG 18,NC
FKEYCFG 19,NC
FKEYCFG 20,NC
FKEYCFG 21,NC
FKEYCFG 22,NC
FKEYCFG 23,NC
FKEYCFG 24,NC
FKEYCFG 25,NC
FKEYCFG 26,NC
FKEYCFG 27,NC
FKEYCFG 28,NC
FKEYCFG 29,NC
FKEYCFG 30,NC
FKEYCFG 31,NC
FKEYCFG 32,NC

```

Local station feature keys
configuration:

- Port number
- Feature key number
- Feature name
- DN (if

Trunk group configuration:

- Trunk group number
- Trunk access code

```

TRKGRPCFG 1,E,#61,4.0.0 4.0.1,8739
TRKGRPCFG 2,D,#62,1.0.0 1.0.1 2.0.0 2.0.1,4002
TRKGRPCFG 3,D,#63,1.0.0 1.0.1 2.0.0 2.0.1,4004
TRKGRPCFG 4,D,#64,1.0.0 1.0.1 2.0.0 2.0.1,4006
TRKGRPCFG 5,D,#65,1.0.0 1.0.1 2.0.0 2.0.1,4008
TRKGRPCFG 6,D,#66,1.0.0 1.0.1 2.0.0 2.0.1,4010
TRKGRPCFG 7,D,#67,1.0.0 1.0.1 2.0.0 2.0.1,4012
TRKGRPCFG 8,D,#68,1.0.0 1.0.1 2.0.0 2.0.1,4014

```

Item not Configured

Caller ID (not configured)

Remote Office 911x series unit configuration

This section shows the configuration settings for the Remote Office 911x series unit. You can obtain a similar configuration printout by performing a configuration download while connected to the Remote Office 911x series unit.

Note: Configuration settings are separated by commas (.).

Configuration example

This configuration example uses the settings identified in the network diagram shown on page 301.

IPCFG 5.6.7.8,255.255.255.0,5.6.7.9 ← 911x unit's IP interface information:
SYSCFG 1,Node 1 ←

ROUCFG 0,911,#99,#98,D,#97,#96

ACCFG N

RLCDETCFG 254,0,1,E,1.2.3.4,E,6135551234

- IP address
- Subnet mask
- IP gateway

Unit ID and node name

System configuration:

- Emergency service number
- SPRE codes

Host PBX connection information:

- RLC's unit ID
- security information (inbound and outbound security IDs)
- RLC's IP address
- RLC PSTN number

Appendix C

Pin-out tables for RLC Multi-I/O cables

In this appendix

Reading the tables	324
RLC Multi-I/O cable–Basic	325
RLC Multi-I/O cable–Enhanced	327

Reading the tables

When you read the heading, entry, heading, entry, and so on, along a single line in the tables in this appendix, the words form a complete sentence.

For example, the first line of the table below is read as follows:

In pair 1 of bundle W1, the red wire connects pin P1-21 to pin P2-5 and carries the following signal: EN0RXD+.

In pair	of bundle	the	wire connects pin	to pin	and carries the following signal:
1	W1,	RED	P1-21	P2-5	EN0RXD+.
1	W1,	BLK	P1-46	P2-12	EN0RXD-.
2	W1,	WHT	P1-22	P2-6	EN0TXD+.
2	W1,	BLK	P1-47	P2-13	EN0TXD-.

IF the first entry in a row is in column	THEN the final column shows the
four	signal carried between the named pins.
five	function of the named pin.

RLC Multi-I/O cable—Basic

One RLC Multi-I/O cable—Basic (NTDR79xx) ships with each Reach Line Card (RLC). This cable provides the following connectivity:

- P1—the switch's I/O panel
- P2—an external (user) Ethernet port
- P3—serial port to admin PC

If you lose your RLC Multi-I/O cable—Basic, contact your Nortel Networks distributor and request order number A0795280 to purchase a new one.

Pin-out information

The following table shows the pin-out of the RLC Multi-I/O cable–Basic:

In pair	of bundle	the	wire connects pin	to pin	and carries the following signal:
1	W1,	RED	P1-21	P2-5	EN0RXD+.
1	W1,	BLK	P1-46	P2-12	EN0RXD-.
2	W1,	WHT	P1-22	P2-6	EN0TXD+.
2	W1,	BLK	P1-47	P2-13	EN0TXD-.
				P2-4	GND (SHD)
1	W2,	RED	P1-17	P3-3	MMIRXD.
1	W2,	BLK	P1-42	P3-2	MMITXD.
2	W2,	WHT	P1-45	P3-5	GND.
2					
			P3-1	P3-4	MMIDTR-MMIDCD
			P3-4	P3-6	MMIDTR-MMIDSR
			P3-7	P3-8	MMIRTS-MMICTS

RLC Multi-I/O cable—Enhanced

The RLC Multi-I/O cable—Enhanced (NTDR80xx) is a 6-plug cable that provides the following connectivity:

- P1—the switch's I/O panel
- P2—an external (user) Ethernet port
- P3—a serial port to admin PC
- P4—the switch's internal Ethernet port
- P5—the cross-connect to local telephones
- P6— (for future use)

You must order this cable separately by contacting your Nortel Networks distributor and requesting order code A0795281.

Pin-out information

The following table shows the pin-out of the RLC Multi-I/O cable—Enhanced:

In pair	of bundle	the	wire connects pin	to pin	and carries the following signal:
1	W1,	BLK	P1-21	P2-5	EN0RXD+.
1	W1,	RED	P1-46	P2-12	EN0RXD-.
2	W1,	BLK	P1-22	P2-6	EN0TXD+.
2	W1,	WHT	P1-47	P2-13	EN0TXD-.
				P2-4	GND (SHD).
1	W2,	BLK	P1-17	P3-3	SDIRXD.
1	W2,	RED	P1-42	P3-2	SDITXD.
2	W2,	BLK	P1-45	P3-5	GND.
2	W2,	WHT			
			P3-1	P3-4	SDIDTR-SDIDCD.
			P3-4	P3-6	SDIDTR-SDIDSR.
			P3-7	P3-8	SDIRTS-SDICTS.
1	W3,	BLK	P1-23	P4-5	EN1RXD+.
1	W3,	RED	P1-48	P4-12	EN1RXD-.
2	W3,	BLK	P1-24	P4-6	EN1TXD+.
2	W3,	WHT	P1-49	P4-13	EN1TXD-.
1	W4,	BLK	P1-1	P5-1	TCMR00.
1	W4,	RED	P1-26	P5-26	TCMT00.

In pair	of bundle	the	wire connects pin	to pin	and carries the following signal:
2	W4,	BLK	P1-2	P5-2	TCMR01.
2	W4,	WHT	P1-27	P5-27	TCMT01.
3	W4,	BLK	P1-3	P5-3	TCMR02.
3	W4,	GRN	P1-28	P5-28	TCMT02.
4	W4,	BLK	P1-4	P5-4	TCMR03.
4	W4,	BLU	P1-29	P5-29	TCMT03.
5	W4,	BLK	P1-5	P5-5	TCMR04.
5	W4,	YEL	P1-30	P5-30	TCMT04.
6	W4,	BLK	P1-6	P5-6	TCMR05.
6	W4,	BRN	P1-31	P5-31	TCMT05.
7	W4,	BLK	P1-7	P5-7	TCMR06.
7	W4,	ORG	P1-32	P5-32	TCMT06.
8	W4,	RED	P1-8	P5-8	TCMR07.
8	W4,	WHT	P1-33	P5-33	TCMT07.
9	W4,	RED	P1-9	P5-9	TCMR08.
9	W4,	GRN	P1-34	P5-34	TCMT08.
10	W4,	RED	P1-10	P5-10	TCMR09.
10	W4,	BLU	P1-35	P5-35	TCMT09.
11	W4,	RED	P1-11	P5-11	TCMR10.
11	W4,	YEL	P1-36	P5-36	TCMT10.
12	W4,	RED	P1-12	P5-12	TCMR11.

In pair	of bundle	the	wire connects pin	to pin	and carries the following signal:
12	W4,	BRN	P1-37	P5-37	TCMT11.
13	W4,	RED	P1-13	P5-13	TCMR12.
13	W4,	ORG	P1-38	P5-38	TCMT12.
14	W4,	GRN	P1-14	P5-14	TCMR13.
14	W4,	WHT	P1-39	P5-39	TCMT13.
15	W4,	GRN	P1-15	P5-15	TCMR14.
15	W4,	BLU	P1-40	P5-40	TCMT14.
16	W4,	GRN	P1-16	P5-16	TCMR15.
16	W4,	YEL	P1-41	P5-41	TCMT15.
1	W5,	BLK	P5-9	P6-2	(reserved)
1	W5,	RED	P5-34	P6-14	(reserved)
2	W5,	BLK	P5-10	P6-3	(reserved)
2	W5,	WHT	P5-35	P6-16	(reserved)
3	W5,	BLK	P5-11	P6-4	(reserved)
3	W5,	GRN	P5-36	P6-5	(reserved)
4	W5,	BLK	P5-12	P6-20	(reserved)
4	W5,	BLU	P5-37	P6-6	(reserved)
5	W5,	BLK	P5-13	P6-8	(reserved)
5	W5,	YEL	P5-38	P6-7	(reserved)
6	W5,	BLK	P5-14	P6-17	(reserved)
6	W5,	BRN	P5-39	P6-9	(reserved)

In pair	of bundle	the	wire connects pin	to pin	and carries the following signal:
7	W5,	BLK	P5-15	P6-24	(reserved)
7	W5,	ORG	P5-40	P6-11	(reserved)
8	W5,	RED	P5-16	P6-15	(reserved)
8	W5,	WHT	P5-41	P6-12	(reserved)

Appendix D

Safety and regulatory information

In this appendix

International safety compliance	334
Electromagnetic compatibility	335
Electromagnetic immunity	336
Electrostatic discharge	337

International safety compliance

The Reach Line Card (RLC) and the Remote Office system comply with international safety regulations as listed on this page.

Underwriters Laboratory (UL)

The RLC complies with and is listed under UL 1950, Third Edition, including revisions based on the Fourth Amendment to IEC 950, Second Edition.

Canadian Standards Association (CSA)

The RLC complies with and is listed under CSA C22.2, No. 950-95.

Europe

The RLC complies with and is listed under EN60950: 1992, incorporating amendments 1, 2, 3, 4 & 11.

Australia

The RLC complies with and is listed under TS001\AS 3260.

Other Countries Deviations Assessed

Refer to Nemko Test Report # 2000 29173.

Electromagnetic compatibility

The Reach Line Card (RLC) does not interfere with operation of other licensed communications systems according to the standards set forth by Australia, the United States, and Canada.

The RLC does not adversely effect the compliance of the Meridian 1 system to:

- AS 3548 Class B (Australia)
- Class A of FCC Part 15, Subpart J
- CSPR B requirements.¹

The margin is at least 2 dB better than the specified limit.

1. CSPR B limits the number of RLCs that can be used in an Option 11 cabinet with the RLC Multi-I/O cable—Enhanced to five (5).

Electromagnetic immunity

The RLC in a Meridian 1 PBX resists electromagnetic interference.

The RLC performs normally when subjected to narrow band radiated fields in frequency range 500 kHz to 1 GHz (field strength up to 10 V/m, 1 kHz, 50% modulated AM signal) per IEC 1000-4-3.

Electrostatic discharge

The Reach Line Card (RLC) is immune to electrostatic discharges typical for an office environment (carpeted floors, low humidity) according to the test method specified by IEC 1000-4-2.

No damage or malfunction occurs when the RLC is exposed to up to $\pm 8\text{kV}$ of direct discharge. An indirect discharge of up to $\pm 16\text{kV}$ does not result in malfunction of the system (to adjacent equipment or connected cabling).

The requirements for both “closed door” and “open door” have been met.

Glossary

10BaseT Ethernet

The Ethernet standard for baseband local area networks using twisted-pair cable carrying 10 megabits per second (Mbps) in a star topology.

A

A-law

A companding technique used in encoding and decoding audio signals in 30-channel pulse code modulated (PCM) systems. A-law companding is the primary method used in Europe. *See also* Mu-law.

adapter

Hardware required to support a particular device. For example, network adapters provide a port for the network wire. Adapters can be expansion boards or part of the computer's main circuitry.

administrator

A user who is responsible for maintaining the RLC or its associated remote units.

agent

A person who is responsible for handling customer calls.

analog

The type of signal used by most telephone connections. A modem converts a digital (computer) signal to analog, and vice versa, so that the signal can travel through telephone lines.

API

See application program interface.

application

A program that runs on a computer.

application program interface

A set of routines, protocols, and tools that programmers use to develop software applications. APIs simplify the development process by providing commonly used programming procedures.

Asynchronous Transfer Mode

A network technology that uses start bits and stop bits (identifying the beginning and end of digital code) to facilitate data transfer. ATM equipment can transmit video, audio, and computer data over the same network, ensuring that no single type of data dominates the line.

ATM

See Asynchronous Transfer Mode.

Automatic Call Distribution (ACD) applications

A separate system or built-in feature of a PBX that equally distributes incoming calls to agents. As calls come in, they are placed into a queue (or a waiting line) for the next available agent. The RLC and its associated remote units support all of Nortel Networks' ACD applications.

B**bandwidth**

The amount of data that the network can transmit, usually expressed in Mbytes per second.

baseboard

See motherboard.

Basic Input/Output System

Flash ROM-based code that runs the Power-On Self-Test (POST) and bootstrap loader. BIOS contains low-level access routines for hardware that can be called from DOS.

basic rate interface

An ISDN subscriber service that uses two B (64Kbps) channels and one D (64 Kbps) channel to transmit voice, video, and data signals.

BIOS

See Basic Input/Output System.

bit

Short for binary digit, the smallest unit of information on a machine. A single bit can hold only one of two values: 0 or 1.

Boolean logic

A logic system that enables a computer to use electricity to make complex decisions. The basic logic gates (And, Or, and Not) determine the flow of electricity through the computer's circuitry and whether specific computing functions are carried out.

boolean

A value that can only be true or false.

branch station

A Meridian Digital Telephone set located at the Remote Office 9110, 9115, or 9150 site.

BRI

See basic rate interface.

bridge

A protocol-independent device that connects two LANs or two segments of the same LAN. Bridges are faster (and less versatile) than routers because they forward packets without analyzing and rerouting messages.

bridge port

Bridge ports are configured on the Remote Office 9150 unit and are used to connect branch office trunks through the host PBX to accommodate conference calls, remote station to remote station calls, and so on.

bus

A collection of wires that connects the microprocessor and main memory to internal computer components. All buses consist of an address bus that transfers data and a data bus that transfers information about where the data should go.

In a network, the bus (also called the backbone) is the main cable that connects all devices on a LAN.

byte

Abbreviation for binary term, a unit of storage capable of holding a single character. On almost all modern computers, a byte is equal to eight bits. Large amounts of memory are indicated in terms of kilobytes (1024 bytes), megabytes (1 048 576 bytes), and gigabytes (1 073 741 824 bytes).

C**cache**

A temporary storage area in computer memory.

call duration timer

Used in PSTN mode only, it specifies the minimum length of time that each call to the host PBX remains open, regardless of telephone activity (or lack thereof).

call on demand

A call connection that is opened only when a connection to the host PBX is required. This is different from a permanent connection, that is open all the time.

call treatment

A method of handling applied to a call while it is waiting to be answered or serviced.

caller ID

Caller ID is used on the RLC to identify the number of the caller requesting access to one of its ports. It is also used on remote units to authenticate incoming calls from the RLC.

calling line identification

An optional service that identifies the telephone number of the caller. This information can then be used to route the call to the appropriate agent or skillset. The caller's telephone number can also be displayed on a phoneset.

card

A thin, rectangular plate that chips and other electronic components are placed on. Examples of cards include motherboards, expansion boards, daughterboards, controller boards, network interface cards, and video adapters.

central processing unit

This is the system unit that holds a PC's essential components.

CBT

See computer-based training.

CD-ROM

A type of optical disk capable of storing large amounts of data (up to 1 Gbyte), although the most common size is 630 Mbytes. A single CD-ROM has the storage capacity of 700 floppy disks and is particularly well-suited to information that requires large storage capacity.

chip

The small flake of silicon crystal that makes up the microprocessor. 2. A type of controller.

CLAN

See customer local area network.

CLID

See calling line identification.

client

The part of a client/server architecture that runs on a personal computer or workstation and relies on a server to perform some operations. For example, an e-mail client is an application that enables you to send and receive e-mail.

COD

See call on demand.

codec

An acronym for COder-DECoder. A device that codes analog signals into digital signals for transmission and decodes digital signals into analog signals for receiving.

COM or COMM

Communications port. This usually refers to the Logical Device name of PC serial ports as defined by DOS.

computer-based training

A type of education that students learn by running special training programs on a computer. CBT is especially effective for training people to use computer applications, because the CBT program can be integrated with the applications.

Configuration Manager

The software application used to configure and administer remote units and the RLC port that they are connected to.

controller board

A special type of expansion board that contains a controller for a peripheral device. When you attach new devices to a computer, such as a disk drive, often a controller board must also be added.

CPU

See central processing unit.

CPU clock

The clock that regulates the execution of instructions inside a computer. *See also* real-time clock.

crash

A serious computer failure whereby the computer stops working or a program closes unexpectedly. A crash indicates a hardware malfunction or a serious software bug.

customer local area network

The LAN that your corporate services and resources connect to. The RLC and its associated remote units both connect to the CLAN.

D**daughterboard**

Usually used as a synonym for an expansion board, a daughterboard is any printed circuit board that connects directly or indirectly to a motherboard.

DB9 connector

A 9-pin connector labeled ADMIN that provides the RS-232 serial port interface. This serial port connection can be used to configure a Remote Office 9150 unit that is directly connected to a PC.

DB25 connector

The DB25 connector on the RLC Multi-I/O cable–Enhanced is for future use.

DC

See direct current.

DHCP

See dynamic host configuration protocol.

digital linear tape

A high-capacity 1/2-inch streaming tape cartridge format.

digital signal processor

A special type of coprocessor that manipulates analog data, such as sound or photographs, that has been converted to digital form.

DIMM

See dual in-line memory module.

direct current

DC, the electrical power used by computers, comes from a single source (such as a battery) that provides a single voltage that stays at a constant level. AC, the power provided by utility companies, must be converted to DC before it can be used in computer systems.

directory number

The number that identifies a phoneset on a switch. The directory number (DN) could be a local extension (local DN), a public network telephone number, or an automatic call distribution directory number (ACD-DN).

DIP

A type of protective packaging for silicon memory chips that provides a safe and convenient means of installing and removing the chip.

DIP switch

A series of tiny switches built into circuit boards that enables you to configure a circuit board for a particular type of computer or application. DIP switches are always toggle switches. This means that they have two possible positions: on or off (or 1 or 0).

direct memory access

DMA speeds up system performance by moving blocks of memory around inside the computer (typically between I/O devices and memory). This process enables the microprocessor to spend its time performing other functions.

DLL

See dynamic link library.

DLT

See digital linear tape.

DMA

See direct memory access.

DN

See directory number.

driver

A program that controls a device. Every device, whether it is a printer, disk drive, or keyboard, must have a driver program. A driver acts like a translator between the device and programs that use the device.

DSP

See digital signal processor.

dual in-line memory module

The protective packaging for microprocessor chips that provides a safe and convenient means of installing and removing the chip.

dynamic host configuration protocol

A protocol for dynamically assigning IP addresses to devices on a network.

dynamic link library

A library of executable functions or data that can be used by a Windows application. Typically, a DLL provides one or more particular functions and a program accesses the functions by creating either a static or dynamic link to the DLL. A DLL can be used by several applications at the same time.

dynamic port pool

A RLC feature that is similar to multiuser ports in that multiple stations can share ports on the RLC. However, users sharing ports from a dynamic pool are assigned to the first available port on the RLC.

E**ECC**

See error correction code.

ECP

See extended capabilities port.

EEPROM

See electronically erasable programmable read-only media.

EIDE

See enhanced IDE.

EISA

See extended industry standard architecture bus.

ELAN

See embedded local area network.

electronically erasable programmable read-only media

A memory chip that needs only a higher than normal voltage and current to erase its contents. An EEPROM chip can be erased and reprogrammed without taking it out of its socket. An EEPROM chip gives a computer and its peripherals a means of storing data without the need for a constant supply of electricity.

electrostatic discharge

Discharge of a static charge on a surface or body through a conductive path to ground. Can be damaging to integrated circuits.

embedded local area network

This is the network connection from the host PBX to the RLC. It is an Ethernet LAN that is segmented from the rest of the Ethernet network and enables signaling and administration access to the RLC. Nortel Networks recommends the following:

- IP traffic should not be routed between the main network and the ELAN.
- An IP route should not be established between the two LANs.

Emergency Service Number

The Remote Office 9150 unit allows you to program an emergency service number (such as 911).

EMI

Electro-magnetic interference. Interference in signal transmission or reception caused by the radiation of electrical and magnetic fields.

enhanced IDE

An IDE hard disk interface enhanced with hardware and firmware changes to support disks larger than 540 Mbytes, four disks instead of two, and faster transfer rates. *See also* IDE.

enhanced parallel port

A parallel port standard for PCs that supports bidirectional communication between the PC and attached devices (such as a printer).

EPP

See enhanced parallel port.

error correction code

A scheme that can detect and fix single-bit memory errors without crashing the system. Also known as Error Detection and Correction (EDAC).

ESD

See electrostatic discharge.

Ethernet

A widely used LAN protocol that uses a bus topology and supports data transfer rates of 10 Mbps.

event

An occurrence or action on the RLC or remote unit, such as the sending or receiving of a message, the opening or closing of an application, or the reporting of an error. Some events are for information only, while others can indicate a problem.

expansion board

Any board that plugs in to one of the computer's expansion slots. Expansion boards include controller boards, LAN cards, and video adapters.

expansion bus

Enables expansion boards to access the microprocessor and memory. *See also* bus.

expression

A building block of a script, used to test for conditions, perform calculations, or compare values within scripts. *See also* logical expression, mathematical expressions, and relational expression.

extended capabilities port

A parallel-port standard for PCs that supports bidirectional communication between the PC and attached devices (such as a printer).

extended industry standard architecture bus

A 32-bit bus that accommodates ISA PC boards.

F**first-level threshold**

The value that represents the lowest value of the normal range for a given field in a threshold class. The system tracks how often the value for the field falls below this value.

G

G.711

G.711 is the international standard for encoding telephone audio on a 64 Kbps channel. It is a pulse code modulation (PCM) scheme operating at an 8 kHz sample rate, with 8 bits per sample. According to the Nyquist theorem, that states that a signal must be sampled at twice its highest frequency component, G.711 can encode frequencies between 0 and 4 kHz. Telcos can select between two different variants of G.711: A-law and μ -law. A-law is the standard for international circuits.

G.726

G.726 is a standard ADPCM algorithm specified by the International Telecommunication Union (ITU) for reducing the 64 kbps A-Law or μ -law logarithmic data of a normal telephone line to 16, 24, 32, or 40 kbps.

G.729

G.729 is a voice compression International Telecommunications Union (ITU) standard that can be used in a wide range of applications including wireless communications, digital satellite systems, packetized speech, and digital leased lines. G.729 provides 8 Kbps bandwidth for compressed speech at toll quality (equivalent to G.726 32 Kbps ADPCM under clean channel condition).

gateway

A device that functions as a node on two or more networks, forwarding packets from one network to addresses in the other networks. In Remote Office context, the gateway is the device on the network that directs traffic to and from the Remote Office 9150 unit or RLC.

Gbyte

See gigabyte.

general protection fault

A computer condition that causes a Windows application to crash. GPFs usually occur when one application attempts to use memory assigned to another application.

gigabyte

1 073 741 824 bytes. One Gbyte is equal to 1024 Mbytes.

GPCP

General purpose computing platform

GPF

See general protection fault.

graphical user interface

The information displayed on the monitor when a Windows application (or another non-command-based application) runs. A graphical user interface uses features such as pointers, icons, I-beams, and menus to make the program easier to use.

GUI

See graphical user interface.

H

handshaking

A process involved in establishing a valid connection or signal between two pieces of hardware or communications software.

host call appearance key

An assigned key on the telephone set at the remote site that is used to establish a connection with the host PBX or to receive incoming calls from the host PBX.

host-controlled call mode

When a call is placed to someone at the host site, or when someone from the host site calls the remote site, the call is in host-controlled call mode. Calls in host-controlled mode are routed through the host PBX.

host station

A telephone set located at the host PBX site.

host trunk

The ISDN PRI or TI connection located at the host site. Host trunks are used to route calls from the host PBX to remote sites over the PSTN.

hub

A common connection point for all 10BaseT cables connected to a small network. A hub enables data to go from one device to another.

icon

A small picture that represents an object or program in a graphical user interface.

IDE

Commonly used to describe the AT attachment design, the dominant hard disk interface. IDE is a cost-effective interface technology for mass storage devices that the controller is integrated into the disk or CD-ROM drive in.

idle timer

Identifies the maximum length of time that an ISDN connection should remain idle before it can be closed. Idle means that a voice connection does not exist, and buttons are not being pressed on the digital telephone.

Industry Standard Architecture

A 16-bit standard interface for add-in cards.

input/output

Refers to any operation, program, or device that enters data into a computer or extracts data from a computer.

integrated services digital network

A worldwide digital communication protocol that permits telephone networks to carry data, voice, and other source material. There are two kinds of ISDN lines—Primary Rate Interface (PRI) and Basic Rate Interface (BRI). *See also* BRI.

internet protocol

The protocol within TCP/IP that governs the breakup of data messages into packets, the routing of the packets from sender to destination network, and the reassembly of the packets into the original data messages at the destination.

I/O

See input/output.

IP

See internet protocol.

IP address

Internet Protocol address. An identifier for a computer or device on a TCP/IP network. Networks use the TCP/IP protocol to route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be 0–255. For example, 1.160.10.240 could be an IP address.

IPX

Internetwork Packet Exchange. A networking protocol used by the Novell NetWare operating systems.

ISA

See Industry Standard Architecture.

ISDN

See integrated services digital network.

J**jumper**

A metal bridge that closes an electrical circuit. Typically, a jumper consists of a plastic plug that fits over a pair of protruding pins. Jumpers are sometimes used to configure expansion boards. By placing a jumper plug over a different set of pins, you can change a board's parameters.

K**Kbyte**

See kilobyte.

kilobyte

1024 bytes. Roughly the amount of information in half a typewritten page.

L**LAN**

See local area network.

LCD

Liquid crystal display. An alphanumeric display using liquid crystal sealed between two pieces of glass.

LED

Light emitting diode. A semiconductor diode that emits light when a current is passed through it.

local area network

A computer network that spans a relatively small area. Most LANs connect workstations and personal computers and are confined to a single building or group of buildings.

local call

A call that originates at your site.

local call appearance key

An assigned key on the telephone set at the remote site that is used to call another station at the branch office, or to place and receive calls through the local PSTN.

local station

A telephone set located at a remote site.

locally controlled call mode

When you place a call from a specified local call appearance key, or your call is to another telephone at your branch site, you are in locally controlled call mode. Calls in locally controlled mode are routed through the local PSTN.

logical expression

A symbol used in scripts to test for different conditions. Logical expressions are AND, OR, and NOT. *See also* mathematical expressions and relational expression.

M

M1

Meridian 1 PBX

MAT

Meridian Administration Tools. This is a Nortel Networks software application that is used to administer the Meridian 1 PBX.

mathematical expressions

The expressions used in scripts to add, subtract, multiply, and divide values. Mathematical expressions are addition (+), subtraction (-), division (/), and multiplication (*). *See also* logical expression, relational expression.

Mbyte

See megabyte.

megabyte

A unit of measurement for data storage equal to 1 048 576 bytes.

megahertz

One million cycles per second.

MHz

See megahertz.

motherboard

The principal board that has connectors for attaching devices to the bus. Typically, the motherboard contains the CPU, memory, and basic controllers for the system. On PCs, the motherboard is often called the system board.

MTBF

Mean time between failures.

Mu-law

A companding method for encoding and decoding audio signals in 24-channel pulse-code-modulated (PCM) systems. Mu-law is the method used in North America and Japan *See also* A-law.

multiuser ports

A Remote Office 9150 unit port feature that allows multiple stations to time-share a single port on the host PBX. All stations that use a multiuser port are always assigned to the same port number (TN) on the host PBX.

N**NetBeui**

See NetBIOS enhanced user interface.

NetBIOS

See Network Basic Input Output System.

NetBIOS enhanced user interface

An enhanced version of the NetBIOS protocol used by network operating systems such as LAN Manager, LAN Server, Windows for Workgroups, Windows 95 and Windows NT.

Network Basic Input Output System

An application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities.

network interface card

An expansion board that enables a PC to be connected to a local area network (LAN).

NIC

See network interface card.

node

A device connected to the network capable of connecting to other network devices. For example, the RLC and each remote unit are nodes on the network.

NPA

See Number Plan Area.

Number Plan Area

Area code

NVRAM

Non-Volatile Random Access Memory. RAM that doesn't lose its memory when you shut the electricity off to it.

O**OA&M**

Operations, administration, and maintenance

object linking and embedding

A compound document standard that enables you to create objects with one application and then link or embed them in a second application.

ODBC

See Open Database Connectivity.

OEM

Original Equipment Manufacturer. The maker of equipment marketed by another vendor, usually under the name of the reseller. The OEM may only manufacture certain components, or complete computers, that are then often configured with software and/or other hardware, by the reseller.

OLE

See object linking and embedding.

online/offline table

The online/offline table is configured on the RLC. It allows you to schedule times that the host PBX connection is made available to the remote site and the times all telephones at the remote site can use only the local telephone service.

The online/offline table is used for controlling ISDN BRI costs.

Open Database Connectivity

A Microsoft-defined database application program interface (API) standard.

Open System Interconnection

A worldwide communications standard that defines a framework for implementing protocols in seven layers.

OS

Operating Standard

OSI

See Open System Interconnection.

P**packetized voice**

Digital signal processors (DSPs), located in the Remote Office 9150 unit and RLC, convert analog voice into digital data. The data is constructed as a UDP/IP voice packet for transmission over an IP network.

parity

The quality of being either odd or even. The fact that all numbers have parity is commonly used in data communications to ensure the validity of data.

parallel port

A type of interface used to connect an external device such as a printer to a PC. Most personal computers have both a parallel port and at least one serial port.

PBX

See private branch exchange.

PC

Personal computer. A computer with an architecture that is compatible with the IBM PC.

pegging

The action of incrementing statistical counters to track system events.

pegging threshold

A threshold used to define a cut-off value for statistics such as short call and service level. Pegging thresholds are used in reports and historical statistics.

personal directory number

A DN that an agent can be reached directly on, usually for private calls.

phoneset

The physical device, connected to the switch, calls are presented to.

PING

Packet Internet Groper. A protocol that can be used to test the Ethernet connection to devices on the network (such as the RLC and its associated remote units).

position ID

A unique identifier for a phoneset, used by the switch to route calls to the phoneset.

POST

See power-on self-test.

power-on self-test

Initializes and performs rudimentary tests on baseboard hardware, including CPU, floating point unit, interrupts, memory, real-time clock, video, and auto-initializing PCI and EISA bus.

priority DN

A user station can be configured as a priority DN. There are two levels of priority—high and normal. High priority level allows you to

- ensure a trunk is always available
- use PSTN trunking for the host PBX connections
- move the high priority DN first from the IP network to the PSTN

private branch exchange

A telephone switch, typically used by a business to service its internal telephone needs. A PBX usually offers more advanced features than are generally available on the public network. Users of the PBX share a certain number of outside lines for placing telephone calls external to the PBX.

protocol

A standard format used for communication between two devices. The protocol determines the type of error checking to be used, the data compression method (if any), how the sending device will indicate that it has finished sending a message, and how the receiving device will indicate that it has received a message.

PSTN

See public switched telephone network.

public switched telephone network

Any common carrier network that provides circuit switching between public users. The term is usually applied to the public telephone network.

Q**QoS Transitioning Technology**

Nortel Networks' patented technology that can automatically switch calls from the IP network to the PSTN when the voice Quality of Service falls below a predetermined threshold, and back to the IP network when the Quality of Service returns to normal.

R**RAM**

Random Access Memory. This is the most common type of memory found in computers and other devices, such as printers. The term RAM is usually synonymous with main memory, the memory available to programs. For example, a computer with 8 Mbytes of RAM has approximately 8 million bytes of memory that programs can use.

RAS

Remote Access Server. A host on the local area network that is equipped with modems to enable users to connect to the network over telephone lines.

real-time clock

A clock that keeps track of the time even when the computer is turned off. *See also* CPU clock.

recorded announcement route

A resource installed on the switch that offers a recorded announcement to callers.

relational expression

An expression used in scripts to test for different conditions. Relational expressions are less than (<), greater than (>), less than or equal (<=), greater than or equal (>=), and not equal (<>). *See also* logical expression and mathematical expressions.

Remote Access Services

A feature built into Windows NT and Windows 95 that enables users to log in to an NT-based LAN using a modem, X.25 connection, or WAN link. Also known as Dial Up Networking.

remote station

A telephone set located at the Remote Office 9150 or Remote Office 911x series site.

remote trunk

From the RLC's point of view, remote trunks are the ISDN BRI connections between the PSTN and the remote unit located at the branch office site.

RJ-11 Connector

A six-conductor modular jack that is typically wired for four conductors. The RJ-11 jack is the most common telephone jack in the entire world.

RJ-45 Connector

An eight position, eight conductor modular jack used for data transmission over a standard telephone wire. The RJ-45 jack provides the 10BaseT Ethernet connection.

RLC

An abbreviation for Reach Line Card. The RLC is installed on the host PBX and relays voice and signaling information from the digital telephones connected at a remote site to the host PBX.

ROM

Read-Only Memory. This is the computer memory that data has been prerecorded on and cannot be removed from.

router

A device that connects two LANs. Routers are similar to bridges but provide additional functionality, such as the ability to filter messages and forward them to different places based on various criteria.

RTC

See real-time clock.

S**SCA**

See single connector architecture.

second-level threshold

The value used in display thresholds that represents the highest value of the normal range for a given statistic.

security identifier

The remote unit sends the branch office security identifier (password) to the RLC for each connection request. The RLC matches the identifier configured for the RLC port. When it finds a match, it grants access to the port and allows the call to proceed.

sequenced packet exchange

A transport layer protocol (layer 4 of the OSI Model) used in Novell Netware networks. The SPX layer sits on top of the IPX layer (layer 3) and provides connection-oriented services between two nodes on the network. SPX is used primarily by client/server applications.

serial port

A general-purpose interface that can be used for almost any type of device, including modems, mice, and printers (although most printers are connected to a parallel port). Most serial ports on personal computers conform to the RS-232C or RS-422 standards.

server

A computer or device on a network that manages network resources. Examples of servers include file servers, print servers, network servers, and database servers.

service

A process that adheres to a Windows NT structure and requirements. A service provides system functionality.

Service Control Manager

A Windows NT process that manages the different services on the PC.

service profile identifier

When you order an ISDN line, your phone company provides you with a SPID for every phone number you have.

silence suppression

A feature that prevents packet transmission during periods when there is no voice data present.

SIMM

Single In-line Memory Module. Used on Macs and PCs. A form of chip packaging where leads (pins) are arranged in a single row protruding from the chip.

simple network management protocol

A set of protocols for managing complex networks. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network and then analyzing the responses.

single connector architecture

A method for supplying power and data lines in one connector on hard disks. Provides hot-swap capability.

single-user ports

A RLC port that supports one remote station.

Small Computer System Interface

A standard for connecting and controlling mass storage devices such as CD-ROMS, tape drives, and hard disks.

SNMP

See simple network management protocol.

SPID

See service profile identifier.

SPRE code

A Special Prefix code that is used to initiate use of a host PBX feature. In a Remote Office context, SPRE codes are used to

- toggle a remote site between online and offline modes
- use the paging feature
- switch an analog or ATA equipped station from host-controlled mode to locally controlled mode so that local calls can be made
- register a Remote Office 9150 unit for a multiuser or dynamic port

SPX

See sequenced packet exchange.

SRAM

Static Random Access Memory. A form of RAM that retains its data without the constant refreshing that DRAM requires.

station

A telephone or fax machine located at a remote site.

stop bit

In asynchronous communications, a bit that indicates a byte has just been transmitted. Every byte of data is preceded by a start bit and followed by a stop bit.

subnet mask

A subnet mask is the part of the IP address used to represent a subnetwork within a network. A typical IP address might be 192.210.34.144. Each part of this address is made up of eight bits. The subnet mask identifies to the RLC or remote unit what portion of the IP address represents the network (and subnetwork) and what portion represents the host.

SVGA

Super Video Graphics Adapter. An extension of the VGA video standard.

switch

In a telecommunications network, a switch is the hardware that receives phone calls and provides connections to telephone sets. The switch allows a connection to be established as necessary and terminated when there is no longer a session to support it.

In networks, a device that filters and forwards packets between LAN segments. Switches operate at the data link layer (layer 2) of the OSI Reference Model and therefore support any packet protocol. LANs that use switches to join segments are called switched LANs or, in the case of Ethernet networks, switched Ethernet LANs.

switch resource

A device that is configured on the switch.

T**TAPI**

See telephone application programming interface.

TCP/IP

Transport Control Protocol/Internet Protocol. The communication protocol used to connect devices on the Internet. TCP/IP is the standard for transmitting data over networks.

telephone application programming interface

A term that refers to the Windows Telephony API. TAPI is a changing (i.e. improving) set of functions supported by Windows that allow Windows applications to program telephone-line based devices such as single and multi-line phones (both digital and analog), modems and fax machines in a device-independent manner.

telephony

The science of translating sound into electrical signals, transmitting them, and then converting them back to sound. The term is used frequently to refer to computer hardware and software that perform functions traditionally performed by telephone equipment.

TFTP

See trivial file transfer protocol.

threshold

A value for a statistic that system handling of the statistic changes at.

threshold class

A set of options that specifies how statistics are treated in reports and real-time displays. *See also* pegging threshold.

Token Ring

A PC network protocol developed by IBM. A Token Ring network is a type of computer network whereby all the computers are arranged schematically in a circle.

trivial file transfer protocol

A simplified version of FTP that transfers files but does not provide password protection or user-directory capability. It is associated with the TCP/IP family of protocols. TFTP depends on the connectionless datagram delivery service, UDP.

trunk

A communications link between a PBX and the public central office, or between PBXs. Various trunk types provide services such as Direct Inward Dialing (DID), ISDN, and central office connectivity.

trunk access digits

Trunk access digits are numbers that are used by the remote unit to determine the trunk to use when routing a call. For example, 9 is a common trunk access digit used to obtain an outside line.

trunk groups

A trunk group consists of one or more trunk lines that are logically grouped. You can configure up to eight trunk groups on the Remote Office 9150 unit.

trunk interface modules

Used to route calls over the PSTN. The number of modules you must install on the Remote Office 9150 unit depends on the number of simultaneous calls you want in host-controlled or locally controlled mode.

U**uninterruptible power supply**

A power supply that includes a battery to maintain power in the event of a power outage. Typically, a UPS keeps a computer running for several minutes after a power outage, enabling you to save data that is in RAM and to shut down the computer safely.

UPS

See uninterruptible power supply.

utility

A program that performs a specific task, usually related to managing system resources. Operating systems contain a number of utilities for managing disk drives, printers, and other devices.

V**V.35**

An ITU-T standard describing a synchronous, physical layer protocol used for communications between a network access device and a packet network. V.35 is most commonly used in the United States and in Europe, and is recommended for speeds up to 48 Kbps. In practice, V.35 is used for synchronous transmission up to 2.048 Mbps.

V.35 interface

A Frame Relay network technology used to carry the voice conversation and telephone set control signals over:

- a Frame Relay Access Device to send the voice and signal packets to the Remote Office 9150 unit via a Frame Relay Network
- a Channel Service Unit/Data Service Unit (CSU/DSU) to access a switched 56K line service

voice compression

Prior to transmission, the voice data is compressed; after transmission, the data is converted back to voice data at the destination. Voice compression means that voice consumes less bandwidth, leaving more bandwidth for data or other voice or fax communications.

voice jitter attenuation

A feature that removes the variable delays from the voice packets sent across the IP network, thus avoiding awkward-sounding speech.

Voice over Internet Protocol (VoIP)

Technology that uses the IP data network to carry the voice conversation and telephone set control signals between a remote site and the host PBX.

W**WAN**

Wide area network. A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local area networks (LANs). The largest WAN in existence is the Internet.

Fields index

Symbols

802.1p mapping 161

A

Allocation 169

B

Bandwidth

Extra 180

Priority Reserved 180

Board ID

RLC System Configuration 152

Browse

Software Upload 251

Upload Configuration 205

BW Connection Statistics

IP QoS Status 217

No of Voice Calls on IP 217

No of Voice Calls on PSTN 217

Remote Unit Number 217

Signaling Status 217

Total Up Trunk BW 217

Used IP BW 217

Used Trunk BW 217

C

Call Status 238

Call Type 214

Callback for PSTN 180

Called Number 214

Caller ID button 181

Caller Info Statistics

Call BW 220

Connection ID 220

Current Media 220

Last Transition to IP 220

Last Transition to PSTN 220

Priority 220

Remote ID 220

Start Time 220

Transitions to Circuit 220

Transitions to PSTN 220

Type 220

Close Time 214

COM port number 140

Compression algorithm 167

Compression algorithms 196

Compression rate 166

Cordless support 167

D

Date 154

Day

RLC System Configuration 154

Dedicated PSTN network port 180

Default (button) 123

Device Type 238

DiffServ Codepoint 160

DSP Gain 153

DSP load 196

Duration 214

E

- Enable DN discovery 154
- Enter a node name to recognize the unit 89
- Enter the local IP Address of the unit 89
- Enter the Local IP Gateway of the unit 90
- Enter the Local IP Mask of the unit 90
- Error % 241

F

- Fallback bandwidth 185
- Files of type 133
- Frequency 154

H

- Hardware Statistics
 - Module No 227
 - Module Type 227
 - Status 227
 - Version 227
- Hardware statistics
 - Available Channels 230
 - Available Flex Channels 231
 - Available MIPS 230
 - Available Voice Channels 231
 - Device Number 230
 - In Service 230
 - Module Number 230
 - Name 231
 - Single Dig Dev ID 230
 - Total Channels 230
 - Total Flex Channels 231
 - Total MIPS 230
 - Total Reserved Channels 231
 - Total Tones Channels 231
 - Total Voice Channels 230
- Help (button) 124
- Hour 241

I

- Idle Timer 180
- IDVR Feature 168, 181
- IDVR feature 168, 170
- IDVR Status 170
- IP Address 136, 153
 - IP Configuration 159
 - Remote Unit Configuration 179
 - Software Upload 250
 - Upload Configuration 204
- IP address 160
- IP Bandwidth 179
- IP Configure 179
- IP Gateway 159
- IP gateway 160
- IP network 160
- IP Network Mask 159
- IP Status 178

J

- Jitter Buffer 153

K

- Key Feature 170
- Key Number 170

L

- Login Name 121
- Login Status 238

M

- Management IP Address 159
- Management IP address 160
- Management IP information
 - Disable 160
- Management IP mask 160

Min Call Timer 181
Module Number 196

N

Node name 152
Number of devices 196
Number of Switches before Lockout 185

O

OK (button) 123, 127, 132
Online/Offline button 181

P

Password 121
Port Number 238
Priority
 RLC Port Configuration 166, 167
PSTN Configure 179
PSTN Number
 Remote Unit Configuration 180
 RLC Port Configuration 169
PSTN Status 179

R

Remote ID 214
Retrieve (button) 124, 129, 132
RLC extension to dial 154
Rx Dropped 241
Rx Error 241
Rx Frames 241

S

Save as type 133
Security ID
 Inbound 178

 Outbound 178
Security Level 178
Send (button) 123, 128, 132
Set the Number of Remote Units 91
Set the Unit Number of the Remote Unit 91
Signal Degrade

 Duration 185
 Threshold 185

Signal Recover

 Duration 185
 Threshold 185

Start DN Discovery 155

Start Time 214

statistics

 Call Type 214
 Called Number 214
 Caller Info Statistics field descriptions 220
 Close Time 214
 Duration 214
 Remote ID 214
 Start Time 214
 Status 214
 Trunk Number 214

Status 214

 Disable 153
 Enable 153
 Remote Unit Configuration 178
 Transition QoS Configuration 185

T

TALC ID 153
TAPI support 168
Time
 RLC System Configuration 154
Total Voice Channels 230
Trunk Connection Statistics
 Call Type 214
 Called Number 214
 Close Time 214
 Duration 214
 Remote ID 214

Start Time 214
Status 214
Trunk Number 214
Trunk Number 214
Trunk Support 153
Tx Frames 241
Type 238

U

Unit Number 178
Unit Type 178
UPkts 234
Usage 166

V

VCT Statistics
Call Start Time 223
Connection ID 223
Duration 223
Remote ID 223
RLC Port Number 223

Voice Activity Detection
Disable 152
Enable 152
VoiceFlex button 181

W

Wish to Enable IP Voice Connection to Remote
91
Wish to Enable PSTN Voice Connection to Re-
mote 92

Index

Numerics

- 16-channel board 44
- 25-pair connector 75, 79, 96
- 32-channel board 45
- 802.1p 15
- 911x
 - see* Remote Office 911x unit
- 9150
 - see* Remote Office 9150 unit

A

- ACD applications 24
- adapters
 - data channel
 - compatibility 23
- adding DSP modules 64
- add-on modules
 - compatibility 23
- Admin 234
- administration
 - changing the administration password 198
 - creating a backup configuration file 200
 - restoring the configuration 203
- administration password
 - see* RLC and Configuration passwords
- administration PC 60
- algorithms, G.711, G.726, G.729A 73
- Analog Telephone Adapter (ATA) 23, 106
- ATA data adapters 107
- auto logoff 137

B

- backup
 - creating a backup configuration file 200, 201

- introduction 200
- storing 200
- when to create 200
- bandwidth
 - Bandwidth Connection Statistics screen 215
 - measuring with Bandwidth Connection Statistics 215
- Bandwidth Connection Statistics Bandwidth Connection Statistics screen 215
- Bandwidth Connection Statistics screen 215
- bandwidth utilization 19
- Basic cable 325–326
 - pin-out 326
- blocking
 - dynamic port pooling 16
 - multi-user ports 16

C

- cables
 - connecting the RLC's cables 79
 - connector table for RLC Multi-I/O cable–Basic 75
 - identifying for installation 74
 - NTDR79xx 75
 - NTDR80xx 76
 - overview 9
 - P1, P2, P3, P4, P5, P6 connectors 12, 76
 - planning the routing of 46
 - RLC Multi-I/O cable–Basic 75
 - cable diagram 9
 - description table 10
 - RLC Multi-I/O cable–Enhanced 76, 159
 - cable diagram 11
- call blocking
 - overview 59
 - reducing 59
- call on demand

- overview 20, 55
- Callback for PSTN 176
- Caller ID
 - List of Caller IDs 192
- Caller ID security 102
- caller ID security 17
 - List of Caller IDs 17
- Caller Information Statistics
 - displaying 219
- Caller Information Statistics screen 218
- Canadian Standards Association
 - CSA C22.2, No 950 334
- Canadian Standards Association (CSA) 334
- card slot
 - introduction 104
- CAT5 data cable 97
- catastrophic failure 271
- Channel 234
- clearing logs 211
- Common Features Specification 4
- compatibility
 - ACD applications 24
 - CTI applications 24
 - modules 23
 - PBX hardware and software 3
 - telephone hardware 23
- configuration
 - Callback for PSTN 176
 - DSP Configuration property sheet 194
 - List of Caller IDs 192
 - online/offline table 189, 190
 - QoS Transitioning Technology
 - transition thrashing 182
 - recommendation 300
- RLC
 - DN Discovery 150
 - system configuration 149, 152
 - field descriptions 152–155
- RLC System Configuration
 - DN discovery 149
 - IDVR 149
- samples
 - Meridian 1 data port
 - Meridian 1
 - data port configuration (example) 304, 310
 - Meridian 1 voice port 302, 308, 310
 - Remote Office 9150
 - Remote Office 9150 unit
 - configuration (example) 319, 322
 - RLC 315
- configuration file
 - creating a backup file 200
 - storing 200
- Configuration Manager
 - closing 145
 - command buttons 123
 - configuration
 - downloading 134
 - uploading 134
 - configuration file
 - creating 133
 - opening 133
 - device type, selecting 135
 - file operations
 - description 127
 - diagram 125
- Help
 - Display Logs definitions 265
 - logging off from a unit 142
 - logging on to a unit 136
 - property sheets 123
 - shutdown, performing 143
 - software problems
 - troubleshooting 264
 - symptom descriptions 264
 - system restart, performing 143
 - system tree 122
- Configuration Wizard
 - introduction 83
 - performing a configuration 88
 - starting 84
 - using to perform initial configuration 83
 - what you can configure 83
- configuring host trunk
 - see* host trunk, configuring
- configuring ISDN BRI
 - see* ISDN BRI
- configuring ISDN PRI
 - see* ISDN PRI
- configuring remote and network ports

- see* ports
- configuring RLC system information 152
- configuring the PBX
 - see* PBX, configuring
- configuring the RLC
 - configuring QoS transition technology 182
 - how the online/offline table works 186
 - online/offline table 189
- ports 162
 - bridge 162
 - network 165
 - remote 164
- remote connection configuration 171
- connection
 - checking host-site connections 96
 - what to do if the PING did not work 98
- connection history 137
- connectivity
 - troubleshooting 258
 - PING
 - failure 270
- CSA C22.2, No. 950 334
- CTI applications 24

D

- data adapters
 - ATA
 - remote port configuration 107, 110
 - MCA
 - remote port configuration 107
- data channel adapters
 - ATAs 23
 - line card capacity 24
 - Meridian Digital Telephone IP Adapters 24
 - overview 23
 - Remote Office 911x 24
- data channels adapters
 - MCAs 23
- data network security 56
- data ports
 - configure as MCA adapters 110
- DB-15 connector 79, 80, 97
- DB-9 connector 80
- deregistration 16
- device connectivity 258
- Device Information screen 236
- dialing plans
 - trunks 59
- dial-up trunking
 - bandwidth utilization 19
 - call on demand 20
 - DN priority 21
 - online/offline table 22
 - overview 19
 - QoS transition 19
- DiffServ 15
- Disc 234, 235
- Display Logs
 - definitions 265
- display logs
 - printing to a file 209
 - resizing 210
- DN Discovery 150
- DN discovery 149
 - explained 150
 - Feature keys 151
 - how it works 151
- DN priority
 - overview 21
- Download Configuration 131, 132
- DSP
 - DSP Configuration property sheet 194
 - DSP Statistics screen 228
- DSP application modules
 - add to 16-channel board 45
 - adding overview 64
 - adding to 32-channel board 45
 - handling 72
 - installing
 - see* installing DSP application modules 72
 - overview 8
 - reducing call blocking 59
 - requirement examples 45
 - requirements 45
 - supported algorithms 73
- DSP Statistics screen 228
- dynamic port pooling
 - blocking 16
 - deregistration 16
 - overview 16

registration 16
SPRE code 16

E

echo cancellation 18
electromagnetic compatibility 335
 AS 3548 Class B (Australia) 335
 Class A of FCC Part 15, Subpart J 335
 CSPR B requirements 335
 margin 335
electromagnetic immunity 336
electrostatic discharge 337
EN90650 334
Enhanced cable 327–331
 pin-out 328–331
 plugs 327
environmental requirements 39
environmental conditions 39
equipment 23
Err 234, 235
Ethernet
 checking the connection 97
 Ethernet Interface Statistics screen 232
 IP address on RLC 158
 MAT 159
 port on RLC 159
Ethernet Interface Statistics
 Admin 234
 Channel 234
 Disc 234, 235
 Err 234, 235
 IFC No 234
 IFC Type 234
 In - Octet 234
 LAN Drv 234
 MPkts 234, 235
 MTU Len 234
 Oper 234
 Out - Octet 234
 QLen 235
 Speed 234
 UPkts 234
Ethernet Interface Statistics screen 232
extended digital line card (XDLC) 2, 78, 104

F

failure to operate 271
fast busy 16
Feature keys 151
File Open 127, 132
File Save As 128, 132
firmware
 downloading an upgrade file 247
 performing an upgrade 248
 types of firmware upgrades 247
 upgrade 264, 265

G

G.711, G.726, G.729A 18
GUI
 DSP Configuration property sheet 194

H

hardware
 compatibility 23
 Hardware Statistics screen 224
Hardware Statistics screen 224
Help
 Display Logs definitions 265
host connection management 54
host trunk, configuring
 introduction 102
 ISDN BRI configuration 103
 ISDN PRI configuration 102
host-controlled call mode
 example external corporate call 29, 35
 example internal corporate call 27, 33
host-controlled calls 25

I

I/O panel
 planning installation for 46
identifying why a problem occurred 254
idle timer 20
IFC No 234

- IFC Type 234
 - In - Octet 234
 - incoming calls 25
 - inoperative equipment 271
 - installing DSP application modules
 - determining how many to add 72
 - handling DSP application modules 72
 - introduction 72
 - to install DSP application modules 73
 - installing the hardware
 - required tools 70
 - installing the RLC
 - connecting the RLC's cables 79
 - general safety 70
 - identifying the cables 74
 - indications of proper cable connections 81
 - indications of proper installation 81
 - installing DSP application modules 72
 - installing into the card slot 78
 - installing the software 82
 - preparing for installation 78
 - testing the connection 96
 - unable to log on 81
 - using Configuration Wizard 83
 - verifying the installation 81
 - installing the software
 - required tools 71
 - installing, planning for
 - administration PC 60
 - cable routing 46
 - deployment options 65
 - deployment planning 46
 - DSP requirements 45
 - future growth 64
 - network considerations 58
 - planning forms 47
 - preinstallation preparation 44
 - preparing the site 44
 - RLC requirements 44
 - system resources management 54
 - taking inventory 47
 - telecom manager's installation checklist 47
 - Integrated Digital Voice Recorder (IDVR) 149
 - international safety compliance 334
 - Australia 334
 - Canadian Standards Association 334
 - EN90650 334
 - other 334
 - Underwriters Laboratory (UL) 334
 - Internet Protocol (IP)
 - address 83
 - addressing and routing 58
 - connection
 - Remote Connection Configuration 172
 - default gateway 83
 - IP Configuration property sheet 158
 - position of the RLC in the network 157
 - subnet mask 83
 - IP Adapters
 - see* Meridian Digital Telephone IP Adapter unit
 - IPE modules 3
 - IPE shelves
 - NT8D37AA 78
 - ISDN BRI
 - configuring 103
 - controlling charges 21
 - idle timer 20
 - minimum call duration timer 20
 - with online/offline table 186
 - ISDN PRI
 - configuring 102
- J**
- Jitter Buffer target depth 150
- L**
- LAN Drv 234
 - LEDs
 - LED indicators 7
 - List of Caller IDs 17, 192
 - locally controlled calls 26
 - locally controlled mode
 - example local call 31
 - logging off from a unit 142
 - auto logoff 137
 - logging on to a unit
 - connection history 137
 - default logon ID and password 136

- from Configuration Manager 136
- through serial port 140
- using the serial port 85
- login ID
 - Configuration Manager 198
 - RLC 198
 - unit 136
- logs
 - clearing 211
 - resizing 210
- lost or forgotten passwords 57

M

- MAS
 - see Meridian Application Server
- MAT 159
- MAT, see Meridian Administration Terminal
- MCA adapters 110
- MCA data adapters 107
- Meridian 1
 - software compatibility 4
 - voice port configuration (example) 302, 308, 310
- Meridian 1 Options 11 (C), 11(C)-mini, 11(E), 51(C), 61(C), 71(C) 3
- Meridian Administration Terminal
 - using to connect to MAS 84
- Meridian Administration Tools (MAT) and Configuration Manager 63
- Meridian Application Server
 - establishing connection by MAT 84
- Meridian Communication Adapters (MCAs) 23
- Meridian Digital Telephone IP Adapter
 - PBX support xvii
- Meridian Digital Telephone IP Adapters
 - data channel adapters 24
- minimum call duration timer 20
- modules
 - compatibility 23
- MPkts 234, 235
- MSL-100 xvii
- MTU Len 234
- multi-user ports
 - blocking 16

- overview 16

N

- Nemko Test Report # 2000 29173 334
- network
 - diagram (example) 301
- network considerations
 - call blocking 59
 - introduction 58
 - IP addressing and routing 58
 - network diagram 58
 - quality of service 59
 - trunks and dialing plans 59
- network diagram 58
- network port configuration 165
- network ports
 - configuration 110
 - configuring 106
 - explained 105
 - how the remote and network ports work together 113
- no call security 17
- node password 56
- NT8D37AA 78
- NTDR79xx 75
- NTDR80xx 76

O

- OK 127, 132
- online/offline table
 - changing the online/offline mode 56
 - configuration 189, 190
 - example of 186
 - how the online/offline table works 186
 - how the remote site goes back online 188
 - implications 188
 - multiple offline periods 187
 - overrides 187
 - overview 22
- Oper 234
- Option 11 cabinets 4
- Out - Octet 234
- outgoing calls

overview 25

P

P1, P2, P3, P4, P5, P6 connectors 10, 75

packet loss handling techniques 18

packet voice

echo cancellation 18

packet loss handling techniques 18

silence suppression algorithm 18, 149

Voice Activity Detection (VAD) 18, 149

voice compression 18

voice jitter attenuation buffer 18

password

Configuration Manager

overview 198

node 56

RLC 198

password (for a unit) 136

password, node 56

passwords

lost or forgotten passwords 57

PBX

configuring

card slot 104

host trunk 102

managing host connections 54

MSL-100 xvii

PBX hardware

IPE shelves 4

Option 11 cabinets 4

PBX hardware and software

compatibility 3

PBX hardware and software compatibility 3

hardware 3

Meridian 1 software 4

PBX options

11(C), 11(C)-mini, 11(E), 21(E), 51(C),

61(C), 71(C), 81(C), Meridian 1

Options 3

PBX, configuring

remote and network ports 106

understanding port relationships 105

PC

administering multiple nodes 61

connection options 60

ethernet connection 61

Meridian Administration Tools and

Configuration Manager 63

serial connection 60

TFTP server 62

Windows PC requirements 62

physical features

cables 9

DSP application modules 8

faceplate diagrams 6

introduction 2

IPE vs Option 11 4

LED indicators 7

RLC motherboard 5

PING 268

failure 270

unsuccessful ping 98

pin-out

RLC Multi-I/O cable—Basic 326

RLC Multi-I/O cable—Enhanced 328–331

pin-out tables for RLC Multi-I/O cables 323–331

port and station assignment 65

port sharing options

dynamic port pooling

blocking 16

multi-user-ports

blocking 16

ports

configuration 162

bridge 162

network 165

remote 164

configuring 106

configuring remote and network ports 106

how the remote and network ports work

together 113

network port configuration 110

remote and network ports overview 105

remote ports configuration 106

RLC Port Configuration property sheet 163

understanding port relationships 105

power requirements

Reach Line Card (RLC) 40

Remote Office 9150 units 40

printing the display logs to a file 209

prioritization of voice packets

802.1p 15

DiffServ 15

problems

solving

catastrophic failure 271

connectivity 258

PING failure 270

LEDs as indicators 255, 256

PING procedure 268

software problems 264

symptom descriptions 264

PSTN

configuration

Callback for PSTN 176

with Configuration Wizard 83

PSTN connection

Remote Connection Configuration 174

PSTN mode

implementing 66

introduction 65

Q

QLen 235

QoS transition

overview 19

QoS Transition Configuration sheet 183

QoS Transition Technology

settings 183

QoS transition technology

QoS Transition Configuration sheet 183

QoS Transitioning Technology 182

configuration

transition thrashing 182

configuring 182

in Caller Information Statistics 218

overview 54

QoS Transition Configuration sheet 183

quality of service 15, 59

R

Reach Line Card

LEDs

troubleshooting 255, 256

Reach Line Card (RLC)

changing the administration password 198

configuration (example) 315

configuring the PBX 101

configuring, *see* configuring the RLC

dial-up trunking 19

dynamic port pooling 16

environmental requirements 39

faceplates diagram 6

how the Reach Line card works 25

installing 69

motherboard diagram 5

operational characteristics 15

overview 2

packet voice 18

PBX hardware and software compatibility 3

physical features 2

planning for installation 43

power requirements 40

QoS transition technology 15

security 17

telephone hardware compatibility 23

registration 16

remote configuration

configuring the remote connection settings

177, 195

property sheet 171, 194

remote connection

introduction 171

Remote Connection Configuration property

sheet 171

IP connection 172

PSTN connection 174

security 172

timers 20

Remote Office 911x

data channel adapters 24

Remote Office 911x Series

PBX support xvii

Remote Office 911x series units

ATA data adapters 110

Remote Office 9150 unit

power requirements 40

remote port configuration 164

- data adapters 107
- remote ports
 - configuration 106
 - configuring 106
 - configuring on RLC 164
 - explained 105
 - how the remote and network ports work together 113
- resizing logs 210
- restarting the system
 - when to perform a restart 143
- restore
 - before you begin 203
 - introduction 203
 - upload a configuration file over the IP network 204
- Retrieve 129, 132
- RJ-11 96
- RJ-45 connector 97
- RLC
 - double-wide
 - data channel adapters 24
 - port configuration 162
 - bridge 162
 - network 165
 - remote 164
 - single-wide
 - data channel adapters 24
- RLC firmware
 - upgrade 264, 265
- RLC Multi-I/O cable
 - Basic
 - connector table 75
 - Enhanced
 - connector table 76
- RLC Multi-I/O cable - enhanced 12
- RLC Multi-I/O cable-Basic 9, 10
 - pin-out 326
- RLC Multi-I/O cable-Enhanced 11, 12, 46
 - testing 96
- RLC Multi-I/O cable-Enhanced
 - pin-out 328-331
 - plugs 327
- RLC Multi-I/O cables 327
 - Basic cable 325-326
 - Enhanced cable 327-331

- pin-out tables 323-331
- RLC password
 - changing 199
 - overview 198
- RLC Port Configuration property sheet 163
- RLC System Configuration 149, 152
 - DN Discovery 150
 - DN discovery 149
 - field descriptions 152-155
 - IDVR 149
- RLC System Configuration field descriptions 152-155
- RS-232 75, 76

S

- safety
 - during installation
 - introduction 70
 - precautionary messages 70
- safety and regulatory information 333
 - electromagnetic compatibility 335
 - AS 3548 Class B (Australia) 335
 - Class A of FCC Part 15, Subpart J 335
 - CSPR B requirements 335
 - margin 335
 - electromagnetic immunity 336
 - electrostatic discharge 337
 - international safety compliance 334
 - Australia
 - TS001 AS 3260 334
 - CSA C22.2, No. 950 334
 - EN90650 334
 - other
 - Nemko Test Report # 2000 29173 334
 - UL 1950 334
- Save Report 209
- Save to Flash 129
- SDI port
 - connecting from a remote site 148
 - see also* ports
- second port
- Meridian Administration Tools 159
- security

- administration password 56
- caller ID security 17
 - List of Caller IDs 17
- data network 56
- level 1 17
- level 2 17
- level 3 17
- levels 17
- lost or forgotten passwords 57
- no call security 17
- node password 56
- overview 17, 56
- Remote Connection Configuration 172
- security identifier 17
- security identifier 17
- Send 128, 132
- Send All 128, 132
- serial connection 60
- serial data interface (SDI) 148
- serial port
 - logging on to a unit 85, 140
 - planning for installation 46
- shortages
 - equipment 47
- shutting down the system
 - performing a system shutdown 144
- silence suppression 149
- silence suppression algorithm 18
- software
 - installation or upgrade tools 71
 - installing 82
- software compatibility
 - Meridian 1 PBX 4
- software problems 264
- software upgrades
 - introduction 252
 - performing 252
- special prefix code 16
- Speed (statistic) 234
- SPRE code 16
 - with online/offline table 187, 188
- statistics
 - Bandwith Connection Statistics screen 215
 - Caller Information Statistics screen 218
 - Device Information screen 236
 - DSP Statistics screen 228

- Ethernet Interface Statistics
 - Admin 234
 - Channel 234
 - Disc 234, 235
 - Err 234, 235
 - IFC No 234
 - IFC Type 234
 - In - Octet 234
 - LAN Drv 234
 - MPkts 234, 235
 - MTU Len 234
 - Oper 234
 - Out - Octet 234
 - QLen 235
 - Speed 234
 - UPkts 234
- Ethernet Interface Statistics screen 232
- Hardware Statistics screen 224
- Trunk Connection Statistics screen 212
- VCT Statistics field descriptions 223
- system resources
 - call on demand capability 55
 - host connection management 54
 - introduction 54
 - QoS transition technology 54
 - variable security 56
- system tree 122

T

- TCM telephone interface 24
- telephone hardware
 - compatibility
 - add-on modules 23
- telephone hardware compatibility
 - data channel adapters 23
 - Nortel Networks CTI and ACD applications 24
- TFTP 248
- TFTP server 62
- timer
 - minimum call duration 20
- timers
 - how timers work to control ISDN costs 21
 - idle timer 20

- minimum call duration timer 20
- Remote Connection Configuration 20
- tools
 - hardware installation 70
 - software installation 71
 - software upgrade 71
- transition thrashing 182
- Trivial File Transfer Protocol (TFTP)
 - RLC firmware upgrade 264, 265
- troubleshooting 254
 - before you begin 254
 - catastrophic failure 271
 - connectivity 258
 - PING failure 270
 - device connectivity 258
 - LEDs as indicators 255, 256
 - PING procedure 268
 - software problems 264
 - symptom descriptions 264
- Trunk Connection Statistics
 - introduction 212
- Trunk Connection Statistics screen 212
- trunks
 - dialing plans 59
- TS001 AS 3260 334

U

- UL 1950 334
- Underwriters Laboratory (UL) 334
 - UL 1950 334
- upgrades, performing
 - obtaining the latest upgrade file 247
 - performing a firmware upgrade 248
 - performing a software upgrade 252
 - types of 247
 - upgrades and configuration files 249
 - verifying the firmware and software version 245
 - when to perform a firmware upgrade 249

- upgrading the software
 - required tools 71
- UPkts 234
- Upload Configuration 130, 132
- using Configuration Manager PING 268

V

- VCT Statistics field descriptions 223
- Voice Activity Detection (VAD) 149
- voice compression 18
- Voice Connection Table (VCT)
 - introduction 221
 - VCT Statistics field descriptions 223
- voice jitter attenuation buffer 18
- voice over IP
 - with Configuration Wizard 83
- Voice over IP mode
 - implementing 67

W

- Windows PC requirements 62

X

- XDLC (extended digital line card) 78, 104

Reach Line Card Installation and Administration Guide

Copyright © 2001 Nortel Networks, All Rights Reserved.

Printed in Canada.

All information contained in this document is subject to change without notice. Nortel Networks reserves the right to make changes to equipment design or program components, as progress in engineering, manufacturing methods, or other circumstances may warrant.

*Nortel Networks, the Nortel Networks Logo, the Globemark, Unified Networks, Meridian 1, MSL-100, and Succession Communication Server for Enterprise 1000 are trademarks of Nortel Networks.

MICROSOFT, MS-DOS, and WINDOWS are trademarks of Microsoft Corporation. PROCOMM PLUS is a trademark of Datastorm Technologies, a subsidiary of Quarterdeck Corporation.

Publication number:	555-8421-210
Product release:	1.3
Document release:	Standard 2.1
Date:	October 2001



555-8421-215

Remote Office 9150

Installation and Administration Guide

Product release 1.3.0

Standard 2.0

September 2001

NORTEL
NETWORKS™

NTDR84AB

Remote Office 9150

Installation and Administration Guide

Product release:	1.3.0
Publication number:	555-8421-215
Document release:	Standard 2.0
Date:	September 2001

Copyright © 2001 Nortel Networks, All Rights Reserved

Printed in Canada

All information contained in this document is subject to change without notice. Nortel Networks reserves the right to make changes to equipment design or program components, as progress in engineering, manufacturing methods, or other circumstances may warrant.

*Nortel Networks, the Nortel Networks logo, the Globemark, Unified Networks, Meridian 1, Succession Communication Server for Enterprise 1000, and MSL-100 are trademarks of Nortel Networks.

PROCOMM PLUS is a trademark of Datastorm Technologies, a subsidiary of Quarterdeck Corporation.

MICROSOFT, MS-DOS, WINDOWS, and WINDOWS NT are trademarks of Microsoft Corporation.

FCC: Customer instructions

The Remote Office 9150 unit complies with Part 68 of the FCC rules. On the bottom side of the equipment is a label that contains, among other information, the FCC registration number and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

The Remote Office 9150 unit uses the following standard connections and codes: USOC Code: RJ21X, Facility Interface Code: 02DU5-64, and Service Order Code: 6.0F.

The REN number shown on the label is used to determine the number of devices that can be connected to the telephone line. Excessive RENs on the telephone line can result in the devices not ringing in response to an incoming call. The sum of the RENs should not exceed five (5.0). To be certain of the number of devices that can be connected to a line, as determined by the total RENs, contact the local telephone company.

If the equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service might be required. However, if advance notice is not practical, the telephone company will notify you as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

No repairs can be performed by you. If you experience trouble with this equipment, please contact the following for repair and warranty information:

Nortel Networks
Product Service Center
640 Massman Drive. Nashville, TN 31210
Phone: 1-800-251-1758

If the equipment is causing harm to the telephone network, the telephone company might request that you disconnect the equipment until the problem is resolved.

This equipment cannot be used on public coin phone service provided by the telephone company. Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission, or corporation commission for information.

Industry Canada: Equipment attachment limitation

NOTICE: The Industry Canada Label identifies certified equipment. This certification means that the equipment meets telecommunications network protective, operational, and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). The Department does not guarantee that the equipment will operate to the user's satisfaction.

Before installing this equipment, you should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. You should be aware that compliance with the above conditions might not prevent degradation in service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, can give the telecommunications company cause to request you to disconnect the equipment.

You should ensure, for your own protection, that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution can be particularly important in rural areas.

Caution: You should not attempt to make such connections yourself, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

NOTICE: The Ringer Equivalence Number (REN) assigned to each terminal device provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface can consist of any combination of devices subject only to the requirements that the sum of the Ringer Equivalence Numbers of all the devices does not exceed 5.

Publication history

September 2001

This is the Standard 2.0 issue of the *Remote Office 9150 Installation and Administration Guide* for Remote Office 9150 Release 1.3.0. Support for Succession for Communication Server 1000 has been added along with new and enhanced feature information that was formerly published in the *Remote Office and RLC Release Notes*.

March 2000

This is the Standard 1.0 issue of the *Remote Office 9150 Installation and Administration Guide* for Remote Office 9150 Release 1.0.

Contents

About this document	xiii
About this guide	xiv
Skills you need	xv
Related information products	xvii
Conventions used in this guide	xix
1 Remote Office 9150 description	1
Overview	2
Section A: Product description	7
What is Remote Office 9150?	8
Remote Office 9150 hardware description	11
Add-on modules description	15
Connection options	17
How the Remote Office 9150 unit works	19
Section B: Features description	29
System security	30
Trunking, connection types, and call timers	32
Telephones	35
Voice over IP features	37
Quality of Service transitioning technology	39
Port management	40
Station priority	41
Connection bandwidth	43
Local calling	44
Online/offline table	46
Other supported features	47
Administration software	48
2 Planning for installation	51
Installation checklist	52
Physical environment	56
Administration PC	61
Network considerations	66

Managing trunk connections	70
Station configuration	73
Security	77
Planning for future growth	79
Deployment options	82
Planning the configuration	87
3 Installing the Remote Office 9150 unit	91
General safety	92
Required tools	94
Unpacking and inspecting the equipment	95
Removing the Remote Office 9150 unit cover	97
Installing a trunk interface or DSP application module	100
Mounting the Remote Office 9150 unit	106
Connecting the Remote Office 9150 unit	113
Powering up the Remote Office 9150 unit	119
Installing the software	122
Using the Configuration Wizard to perform initial configuration	124
Testing the network connections	138
4 Configuration Manager overview	143
Starting Configuration Manager	144
Configuration Manager description	147
Using the online Help	155
Configuration files description	156
Working with configuration files	163
Selecting the device type for offline configuration	167
Logging on to a unit	169
Logging off from a unit	176
Performing a system restart or shutdown	177
Closing Configuration Manager	180
Uninstalling the Configuration Manager software	182
5 Configuring the Remote Office 9150 unit	183
Configuring the system settings	184
Configuring International Tones	190
Configuring the Remote Office 9150 unit's IP interface	195
Configuring the RLC connection information	198
Configuring the PSTN connection number	202
Configuring the security level	204

	Configuring trunks and trunk groups	208
	Configuring BRI trunks	211
	Configuring trunk groups	215
	Configuring stations	219
	Defining stations	225
	Configuring a fax station	231
	Configuring DSP resources	235
6	Using Remote Office 9150 stations	239
	Modes of operation	240
	Placing and receiving calls	244
	Indicator updates	248
	Display messages	250
	Telephone features operation	253
	Going online and offline	257
7	Administration	259
	Changing the administration password	260
	Section A: Performing backups and restores	265
	Creating a backup configuration file	266
	Restoring the configuration	268
	Section B: Working with system logs	273
	Displaying logs	274
	Resizing logs	276
	Clearing logs	277
	Section C: Viewing statistics	279
	Trunk Connection Statistics screen	280
	Bandwidth Connection Statistics screen	282
	Caller Information Statistics screen	284
	Hardware Statistics screen	287
	DSP screen	289
	Ethernet Interface Statistics screen	292
	BRI Statistics screen	295
	Local Call Statistics screen	297
	Remote Call Statistics screen	299
	Device Information screen	301
	ISDN Module Information screen	303
	Network Statistics screen	305

Section D: Performing upgrades	309
Verifying the firmware and software version	310
Obtaining the latest upgrade file	312
Extracting upgrade files from the download file	313
Performing a firmware upgrade	315
Performing a software upgrade	320
8 Troubleshooting	321
Before you begin	322
Remote Office 9150 LEDs	323
Digital telephone	325
Device connectivity	330
Software problems	334
Using Configuration Manager's Ping	336
Recovering from a catastrophic failure	339
A Planning forms	341
Overview	342
Completing the Remote Office 9150 forms	344
Configuration Information—Stations	346
Configuration Information—ISDN BRI Modules	350
Configuration Information—Network Connections	353
Configuration Information—Dialing Plans	354
System expansion worksheet	355
B Sample configuration files	359
Example of a network	360
Voice port configuration on the Meridian 1 PBX	362
Data port configuration on the Meridian 1 PBX	364
RLC configuration	366
Remote Office 9150 unit	370
C Connection pin-out tables	373
TELCO 1 connector pin-out table	374
TELCO 2 connector pin-out table	376
Ethernet connector pin-out table	378
Admin (serial) connector pin-out table	379
Power connector pin-out table	380

D	Display log definitions	381
	Display logs	382
	Glossary	445
	Fields index	467
	Index	471

Preface

About this document

In this preface

About this guide	xiv
Skills you need	xv
Related information products	xvii
Conventions used in this guide	xix

About this guide

The *Remote Office 9150 Installation and Administration Guide* describes how to install, configure, and manage the Remote Office 9150 unit in a branch office.

Who should read this guide

This guide is for the following individuals who are responsible for the installation, configuration, and day-to-day management of the Remote Office 9150 unit system:

- Nortel Networks distributors
- telecom network managers and administrators
- data network managers and administrators
- branch office managers and administrators

Assumptions

This document assumes that you have the skills listed on page xv.

How to use this guide

This guide explains, step-by-step, how to install, configure, and use the Remote Office 9150 unit product. To get an overview of what you need to do, review this guide before beginning Remote Office 9150 unit installation and configuration.

When you are ready to begin, follow the steps in the order in which they are presented. This helps you to achieve a successful installation.

Skills you need

This section describes the skills and knowledge you need to use this guide effectively.

Nortel Networks product knowledge

Knowledge of, or experience with, the following Nortel Networks products is helpful when working with the Remote Office 9150 unit:

- the Meridian 1, MSL-100, Succession Communication Server for Enterprise 1000 switches
- Meridian digital telephones

Telecommunications experience

Knowledge of, or experience with, telecommunications is helpful when working with the Remote Office 9150 unit:

- Extended Digital Line Cards (XDLCS) and how they work
- configuring voice and data ports
- configuring ISDN BRI, PRI (or other types of trunks)
- establishing telephone connections

Data networking experience

Knowledge of, or experience with, data networking is required when working with the Remote Office 9150 unit:

- networking fundamentals and concepts
- IP protocol
- network addressing and routing
- network traffic analysis and provisioning
- network security
- Voice over IP (general knowledge)

PC experience or knowledge

Knowledge of, or experience with, the following PC tasks is helpful when administering the Remote Office 9150 unit:

- general knowledge of Microsoft Windows
- software installation
- network configuration

Related information products

This section lists information products where you can find additional information.

Meridian 1 documents

The following documents describe how to establish telephone and trunk connections between the Remote Office 9150 unit and the BIX in-building cross-connect system:

- *Meridian 1 Installation planning* (NTP 553-3001-120)
- *Telephone and attendant console installation* (NTP 553-3001-215)
- *BIX* In-Building Cross-Connect System Material Installation and Servicing (Wall-Mounted System)* (NTP 631-4511-200)

Remote Office 9150 and RLC documents

Remote Office and RLC Release Notes (NTP 555-8421-102)

The *Release Notes* describe the features and known problems for the Reach Line Card (RLC) and Remote Office 9150 branch office system.

The printed copy might supersede the copy provided on the CD-ROM. You can obtain the most up-to-date version by clicking on the Customer Support, Document, North America links at the following website:

www.nortelnetworks.com

Reach Line Card Installation and Administration Guide (NTP 555-8421-210)

This document, written for both the installer and administrator, explains how to install and configure the Reach Line Card on the host PBX.

Installer's Notes

The following Installer's Notes are quick reference documents that are provided with the component discussed in the document:

- *Reach Line Card Installer's Notes*
- *Remote Office 9150 and RLC DSP Application Module Installer's Notes*
- *Remote Office 9150 Trunk Interface Module Installer's Notes*

Each document summarizes the installation and configuration procedures for the component and provides cross-references to other documents for more detailed information.

Note: You cannot order these documents separately.

CD-ROMs

The *Remote Office Product CD-ROM*, contains

- documentation in Adobe Acrobat Reader (PDF) format
- firmware
- Configuration Manager software

How to obtain the product documentation and CD-ROMs

You can order the printed documentation and CD-ROMs from your Nortel Networks distributor.

You can also download the documentation in Adobe Acrobat Reader (PDF) format from the Nortel Networks web site. For more information, refer to the *Remote Office and RLC Release Notes* (NTP 555-8421-102).

Conventions used in this guide

This section describes the conventions used in this guide.

Precautionary messages

Note: A note describes the secondary results of procedures or commands, or special conditions under which you must use a procedure or command.

ATTENTION

Provides information essential to the completion of a task.



CAUTION

Risk of data loss or equipment damage

Cautions you against unsafe practices or potential hazards, such as equipment damage, service interruption, or loss of data.



WARNING

Risk of minor personal injury

Warns you of a potentially hazardous situation that can result in minor or moderate injury.



DANGER

Risk of death or serious personal injury

Alerts you to an immediate hazard that can result in death or serious injury.

**DANGER****Risk of electric shock**

Alerts you to an immediate hazard that can result in death or serious injury through high voltage or electric shock.

How this guide presents instructions for selecting menu options

To simplify the instructions for selecting options from the menu, this guide abbreviates the selection path. For example, if a procedure requires you to choose Over IP from the Remote Connectivity menu, which is under the Tests menu, this guide uses the following style:

From the menu, choose Tests → PSTN Connectivity → Over IP.

How this guide presents instructions for displaying property sheets

To simplify the procedures for accessing property sheets throughout this guide, the instructions for displaying a particular property sheet are summarized in a “Getting there” statement.

The procedure for displaying the screen that you need depends on whether you are

- performing an online configuration (that is, you are connected to a node by serial port or Telnet)
- performing an offline configuration (that is, you are not connected to a node)

Example

Getting there 9150 → Configuration Manager → IP Configuration

The long instruction for this example is shown on the next page.

- 1 Do the following:

IF	THEN
you are performing an offline configuration	select the device type as described in "Selecting the device type for offline configuration" on page 167.
you are performing an online configuration	connect to, and then log on to the node as described in "Logging on to a unit" on page 169.

- 2 In the left pane, click the plus sign beside Configuration Manager to expand the node list.
- 3 Click IP Configuration.

Result: The IP Configuration property sheet for the Remote Office 9150 unit appears in the right pane.

Chapter 1

Remote Office 9150 description

In this chapter

Overview	2
Section A: Product description	7
Section B: Features description	29

Overview

The Remote Office 9150 unit provides full-featured host PBX services to as many as 32 users located in your office.

The Remote Office 9150 solution consists of the following components:

- **Reach Line Card (RLC)**
The RLC is installed in the PBX at the host location and relays voice and signaling information from the digital telephones connected at the Remote Office 9150 site to the PBX at the host site.
- **Remote Office 9150 unit**
The Remote Office 9150 unit is installed in your office. It relays voice and signaling information between the digital telephones in your office to the PBX at the host location.
- **10BaseT Ethernet and ISDN Basic Rate Interface (BRI) connections**
These connections provide the voice and data connections between the Remote Office 9150 unit and the host PBX.
- **ISDN BRI trunk interface modules are supported for the following:**
 - U interface
 - S/T interface
- **optional Digital Signal Processor (DSP) application modules**
You can add these modules to increase the system's voice processing capacity.

Supported platforms

The following PBX platforms support the Remote Office 9150 solution:

- Meridian 1
- MSL-100
- Succession Communication Server for Enterprise 1000

The term "host PBX" refers to any of the above supported platforms.

What does the Remote Office 9150 unit do?

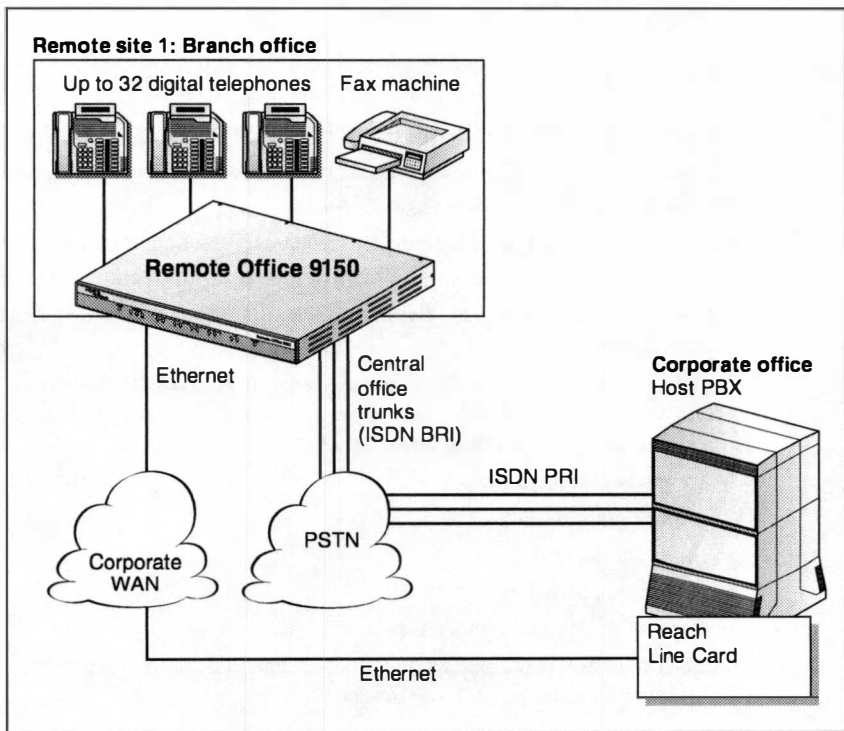
The Remote Office 9150 unit uses the Voice over IP technology to route voice conversation and phoneset control signals between your office and the host PBX over your existing IP data network. The Remote Office 9150 unit can also route calls over the PSTN.

This is accomplished using the following components:

- the Remote Office 9150 unit located in your office
- the RLC located on the PBX at the host site

These two components, along with the 10BaseT Ethernet and ISDN BRI connections, extend the host PBX services to users in your office.

The illustration below shows the connection between a Remote Office 9150 unit and an RLC.



Note: Nortel Networks does not support a Remote Office system as a free-standing key system.

Telephone call modes

Calls can be placed through the Remote Office 9150 unit in any of the following modes:

- **host-controlled mode**
When a call is processed through the host PBX, the call is in host-controlled call mode. The call can be routed over the IP network or the PSTN.
- **locally controlled call mode**
When a call is processed through the local PSTN, the call is in locally controlled call mode.

Product features

The Remote Office 9150 unit offers the following features:

- **system security that supports three security levels—no security, calling line identification (CLID), and security identifier**
- **trunking allocation that automatically allocates trunk bandwidth as it is needed**
- **support for Meridian digital telephones, telephone modules, and standard calling features**
- **Voice over IP features that automatically switch from the IP network to the PSTN when the voice Quality of Service (QoS) falls below a predetermined threshold, and back to the IP network when the QoS returns to normal**
Voice packet features include:
 - **voice compression**
 - **jitter attenuation**
 - **silence suppression.**
- **permanent or demand connection**
If the connection is defined as on demand, then you can configure minimum call duration and idle timers.

- single user ports, multi-user ports, and dynamic port pooling that assigns users to the first available port
- the ability to ensure QoS for specific users

This is done by assigning more priority to those users. There are four levels of priority:

 - high
 - normal
 - IP only
 - circuit-switched only
- the ability to set the Differentiated Services (DiffServ) code-point to Nortel Network's standards for Voice over IP and add the 802.1p priority header
- local calling that allows you to place calls to other extensions within your office, or to telephones in your local community
- Bridge ports to allow you to use Call Forward, Transfer and Conference PBX features with local incoming PSTN calls
- an online/offline table that is configured on the RLC for scheduling periods of times during which:
 - the ISDN BRI connection to the host PBX is made available to the Remote Office 9150 site

Note: When the Remote Office 9150 unit is in offline mode, calls cannot be made or received through the host PBX over the IP or PSTN.
 - all telephones in your office can use only the local PSTN service

This allows you to ensure that unwanted ISDN BRI telephone calls through the host PBX are disabled after business hours.
- an emergency service number that can be programmed with your local emergency number
- an analog port that can send and receive faxes
- 56/64K dynamic adaptation to detect and adjust bandwidth
- support for NAT routers
- administrative capabilities that allow you to perform a variety of administrative tasks, such as:
 - changing the administration password
 - making configuration changes

- viewing the system logs and statistics
- performing upgrades, backups, and restores

Section A: Product description

In this section

What is Remote Office 9150?	8
Remote Office 9150 hardware description	11
Add-on modules description	15
Connection options	17
How the Remote Office 9150 unit works	19

What is Remote Office 9150?

Remote Office 9150 is a product that provides full-featured host PBX services to as many as 32 users located in your office.

The Remote Office 9150 unit uses the Voice over IP technology to route voice conversation and phoneset control signals between your office and the host PBX over your existing IP data network.

The Remote Office 9150 unit can also use the PSTN to route calls if

- the voice QoS degrades below predefined thresholds
In this case, Nortel Networks' patented QoS transitioning technology automatically transitions calls to the PSTN when the voice QoS degrades. Calls transition back to the IP network when the QoS returns to normal.
- you are not yet ready to use the IP network to route voice calls
You can configure the Remote Office 9150 unit to use only the PSTN, and implement the IP network functionality when you are ready.

This section provides a brief description of each component used in a Remote Office 9150 system.

Reach Line Card

The Reach Line Card (RLC) is installed in the PBX at the host location. The RLC provides service for up to 16 ports on a 1-slot card, or 32 ports on a 2-slot card. It emulates a standard digital line card (XDLC), providing PBX functionality for telephones at remote locations (including sites using the Remote Office 9150 unit).

The RLC relays voice and signaling information between the digital telephones connected at the Remote Office 9150 site to the PBX at the host site. Like the Remote Office 9150 unit, the RLC can route calls over the IP network or the PSTN, or both when the QoS transitioning technology feature is configured.

For a more detailed description, refer to the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210).

Remote Office 9150 unit

The Remote Office 9150 unit installed in your office provides PBX functionality for up to 32 digital telephones. Voice and signaling information between the digital telephones connected at your office and the RLC installed on the PBX at the host location is relayed over one or both of the following:

- IP network
- PSTN

10BaseT Ethernet and ISDN BRI connections

These connections provide the voice and data connections between the Remote Office 9150 unit and the host PBX. See “Connection options” on page 17 for a more detailed description.

Optional trunk interface modules

You can install up to four ISDN BRI U or S/T interface modules in the Remote Office 9150 unit. They provide the interface to the ISDN BRI lines provided by your telephone service provider, and are used to route calls over the PSTN.

Optional Digital Signal Processor application modules

You can install up to three Digital Signal Processor (DSP) application modules to increase the Remote Office 9150 unit's voice processing capacity. (See “Add-on modules description” on page 15).

Configuration Manager

Use the following tools to configure the Remote Office 9150 unit:

- for first-time configuration: Configuration Wizard
The Configuration Wizard provides the ability to configure only the minimum information needed to get the Remote Office 9150 unit up and running.
For more details, see “Using the Configuration Wizard to perform initial configuration” on page 124.
- for ongoing configuration and administration: Configuration Manager
For more details, see the following:
 - Chapter 4, “Configuration Manager overview”

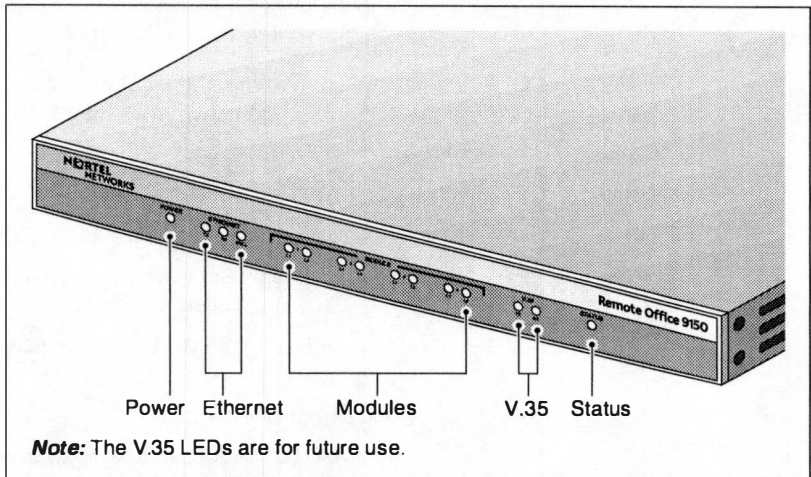
- Chapter 5, “Configuring the Remote Office 9150 unit”
- Chapter 7, “Administration”

Remote Office 9150 hardware description

The Remote Office 9150 unit is installed in your office and can be mounted on a desk, in a rack, or on the wall. This section describes the LED displays, power supply, cables, and connectors for the unit.

LEDs on the Remote Office 9150 unit

The following diagram shows the LEDs on the front panel of the Remote Office 9150 unit.



G101402

The operational status of the Remote Office 9150 unit is indicated by these LEDs as described in the following table.

LED type	LED name	Description
Power	On	When lit, this LED indicates that power is present.
Ethernet	TX	When flashing, this LED indicates that data is being transmitted by the Remote Office 9150 unit over the Ethernet network.
	RX	When flashing, this LED indicates that data is being presented to the Remote Office 9150 unit over the Ethernet network.
	COLL	When flashing, this LED indicates that a collision has occurred on the Ethernet network.
Module	L1 and L2	L1 LED: ■ not lit: there is no D-channel activity ■ flashing: the D-channel is active but the B-channel is not active ■ lit solid: both the D- and B-channels are active
		L2 LED: ■ not lit: the B-channel is not active ■ lit: the B-channel is active
V.35	TX	For future use.
	RX	For future use.
Boot status	Status	Indicates the condition of the Remote Office 9150 unit. This LED stays lit when the power on self-test is successful. If it goes out, there is a problem.

Note: Since Ethernet traffic has a nominal speed of 10 Mbps, the flashing Ethernet COLL, TX, RX LEDs are cosmetic. They do not reflect real-time traffic patterns or packets.

Connectors

The following connections are made from the rear panel of the Remote Office 9150 unit to the telephone and data networks:

- Two 25-pair connectors (labeled TELCO 1 and TELCO 2) provide tip and ring connections to user stations (telephones) and central office trunks (ISDN BRI).

These connections provide the interface to the telephone network and the Public Switched Telephone Network (PSTN).

- An RJ-45 connector (labeled ETHERNET) provides a 10BaseT Ethernet connection.

This connection provides the ability to pass both voice and data traffic over the existing Ethernet network.

- A DB-9 connector (labeled ADMIN) provides an RS-232 serial port connection.

You can use this serial port connection to configure a Remote Office 9150 unit that is directly connected to a PC.

- The DB-25 connector (labeled V.35) is for future use.

Refer to Chapter 2, "Planning for installation," for a detailed description of cables and connectors.

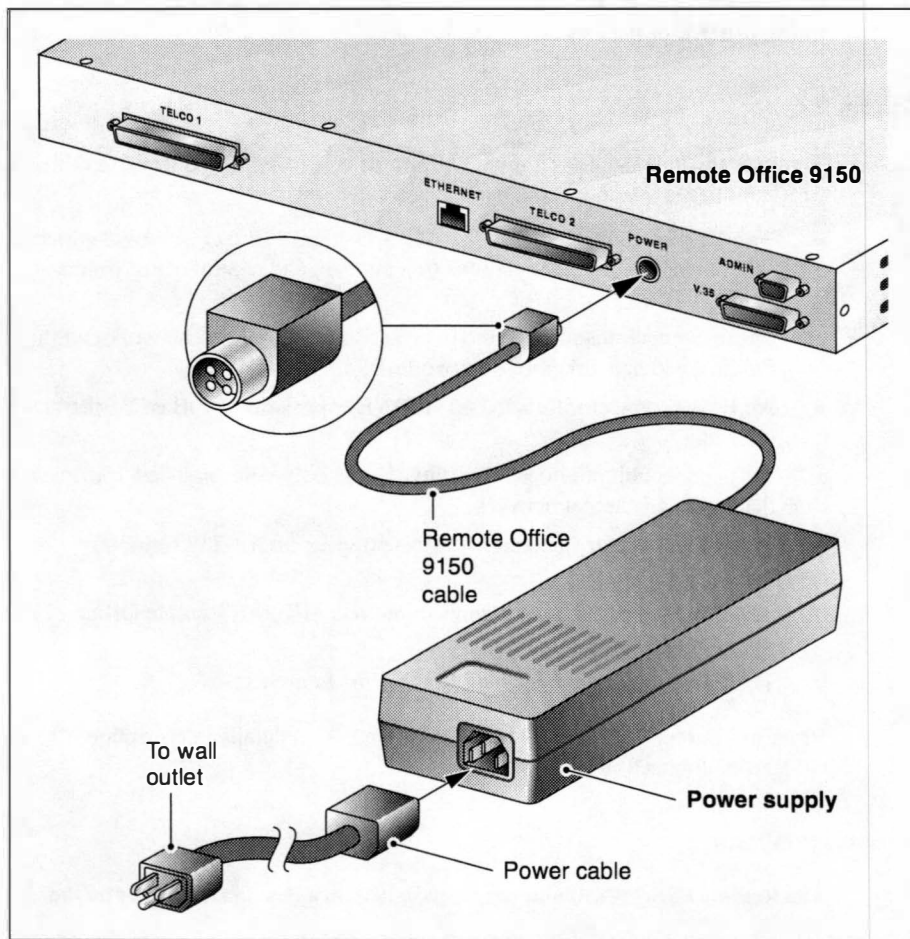
Mounting options

The Remote Office 9150 unit can be mounted on a desk, in a rack, or on the wall.

Universal power supply

The Remote Office 9150 unit includes an auto-sensing 110/220 V power supply that is compatible with commercially available UPS systems. See the diagram on page 14.

Remote Office 9150 power supply



Add-on modules description

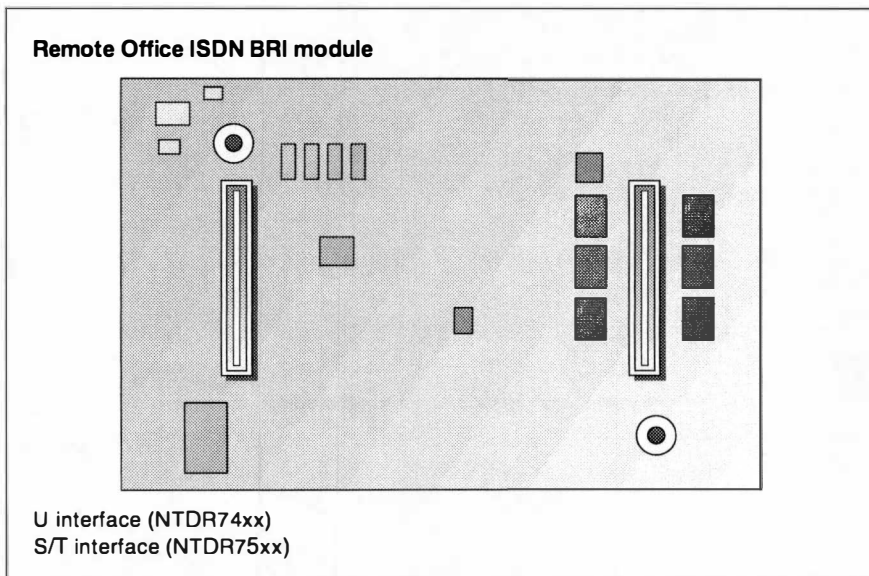
The Remote Office 9150 unit can support trunk interface modules, such as ISDN BRI U or S/T interfaces, and up to three DSP application modules.

Optional trunk interface modules

The Remote Office 9150 unit can support up to four U or S/T ISDN BRI interfaces. Each module supports one ISDN BRI line (with two B-channels) from the local telephone service provider.

Initially, the Remote Office 9150 unit ships with no ISDN BRI modules installed.

ISDN BRI module



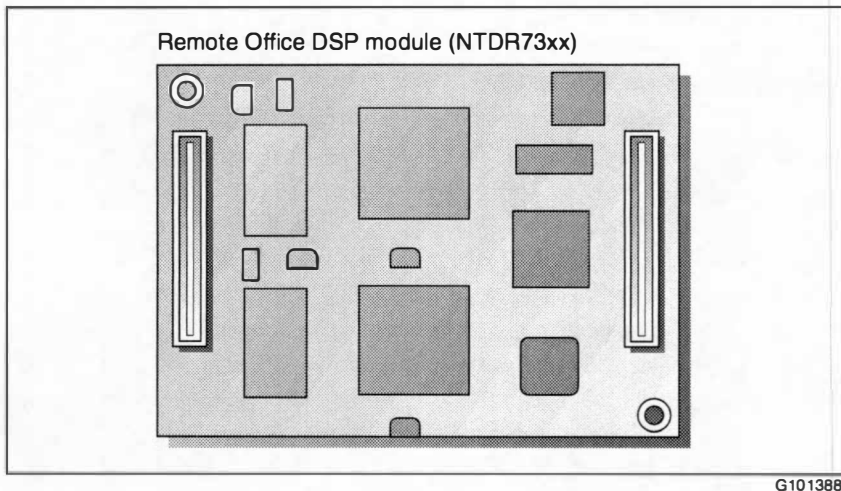
G101420

Optional DSP application modules

DSPs convert voice and fax into digital data for transport over the IP and PSTNs. Initially, the Remote Office 9150 unit ships with the ability to support up to eight simultaneous calls through a DSP that is built into the Remote Office 9150 unit's motherboard. To add support for up to 32 simultaneous calls, you must install DSP application modules. Up to three DSP application modules are supported. Each module provides up to eight more simultaneous calls.

In addition, you can configure the Remote Office 9150 unit for blocking with only enough modules to support the maximum number of simultaneous calls. For example, a Remote Office 9150 unit that is equipped with a single DSP application module supports 16 simultaneous calls, for a ratio of 2:1 blocking. For more details, see "Planning for future growth" on page 79.

DSP application module



Connection options

Communications between the Remote Office 9150 unit in your office and the host PBX take place using 10BaseT Ethernet or ISDN BRI connections, or both. This section provides a description of each of these connections.

10BaseT Ethernet interface

Voice over IP technology is used to carry voice conversation and phoneset control signals over your IP network to the host PBX. The voice data is forwarded as UDP/IP packets, and the signaling data is forwarded as TCP/IP packets.

ISDN BRI lines to PSTN

The PSTN provides a cost-effective alternative to leased lines. You can use ISDN BRI lines at the Remote Office 9150 site to make local calls without involving the host PBX. You can also choose to use the ISDN BRI lines instead of the IP network to route calls through the host PBX.

To use ISDN BRI lines, you must install trunk interface modules. The Remote Office 9150 unit can support up to four U or S/T ISDN BRI trunk interface modules. (See “Add-on modules description” on page 15.)

Quality of Service transitioning technology

If both the IP network and ISDN BRI lines are used, you can use the QoS transitioning technology to reroute calls from the IP network to the PSTN when the QoS on the IP network degrades. When the QoS returns to normal, the QoS transitioning technology automatically moves the calls back to the IP network.

The Remote Office 9150 unit monitors the QoS on the IP network. If the QoS falls below preprogrammed acceptable thresholds, calls are dynamically and transparently switched to the ISDN BRI lines. See “Quality of Service transitioning technology” on page 39 for additional details.

Analog port for fax machines

The Remote Office 9150 unit has one analog port that you can use as a fax connection. See “Fax support” on page 47 for more detailed information.

How the Remote Office 9150 unit works

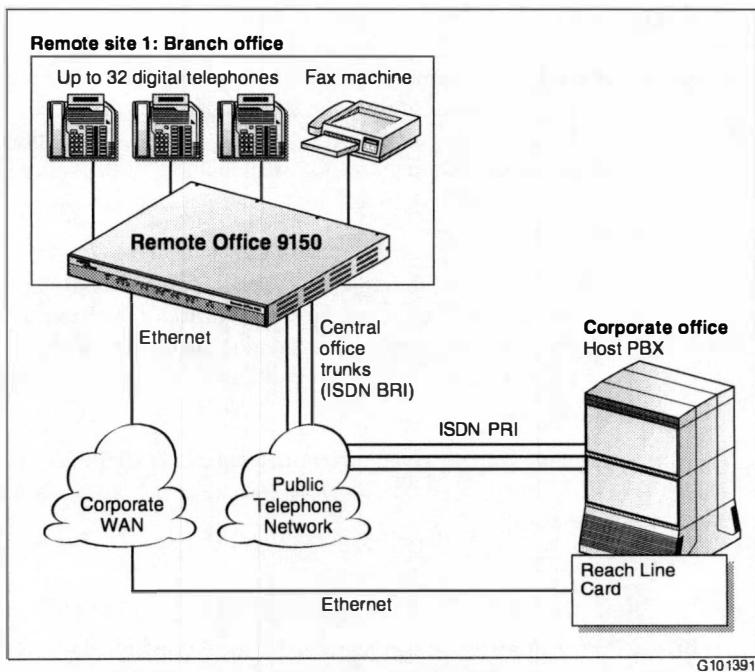
There are two major components to the Remote Office 9150 product:

- the Remote Office 9150 unit located in your office
- the RLC located on the PBX at the host site

These two components, along with the connection options described on page 17, extend the host PBX services to users in your office.

Network diagram

The following diagram shows a RLC and Remote Office 9150 network.



Outgoing call process

To place outgoing calls, users can either pick up the handset on the telephone or press a line appearance key. There are two types of line appearance keys:

- host call appearance key
Use this key to make a call through the host PBX.
- local call appearance keys
Use these keys to make calls to other stations in your office, or to make and receive calls through the local PSTN. You can define up to two local call appearance keys on each digital telephone.

For a detailed description of the outgoing call process, see the sample illustrations beginning on page 22.

Incoming call process

When a user places a call through the host PBX to a user at the Remote Office 9150 site, a connection is made from the RLC to the Remote Office 9150 unit and the host PBX completes the call. If a connection cannot be established, then the call rings until it is forwarded to voice mail by the host PBX. See Chapter 6, “Using Remote Office 9150 stations,” for a more detailed description of the incoming call process.

When someone places a call through the PSTN to a user at the Remote Office 9150 site, a connection is made from the central office to the Remote Office 9150 unit. The number that outside callers dial is the number assigned by the ISDN service provider to the ISDN BRI B-channel on which the incoming call is received.

You can configure an unanswered incoming local call to Call Forward to a DN on the host PBX. The Bridge Port connects the call to the host PBX and it can then transfer to voicemail.

Bridge Port

A Bridge Port is a proxy port that represents a local or inbound PSTN call to the host PBX. When a local incoming call on a Remote Office 9150 unit needs PBX services, the Bridge Port obtains a PBX presence on behalf of the local call.

Bridge Ports can represent the following types of local calls:

- Call Forward: A Local and Remote call made to another Local and Remote telephone uses Call Forward to connect to a third telephone on the PBX.
- Call Transfer: A Local call to a Local and Remote telephone uses Call Transfer to connect to a local trunk or a host-based set.
- Conference: A Remote call to a host telephone can connect to trunk call(s), or if you are on a call to a local trunk, you can connect to host telephone(s) to create three-or-more-party telephone calls.

To configure Remote Office 9150 Bridge Ports refer to page 225.

Host controlled call mode

When a user places a call to someone at the host site, or when someone from the host site calls the Remote Office 9150 site, the call is in host-controlled call mode. Calls in host-controlled mode are routed through the host PBX. See the sample illustrations on pages 22 and 24.

Locally controlled call mode

When a user places a call from a local call appearance key, or the call is to another telephone at the Remote Office 9150 site, the call is in locally controlled mode. Calls that are initiated from the local call appearance key are routed through the local PSTN. Calls to other extensions in the Remote Office 9150 site are routed only through the Remote Office 9150 unit.

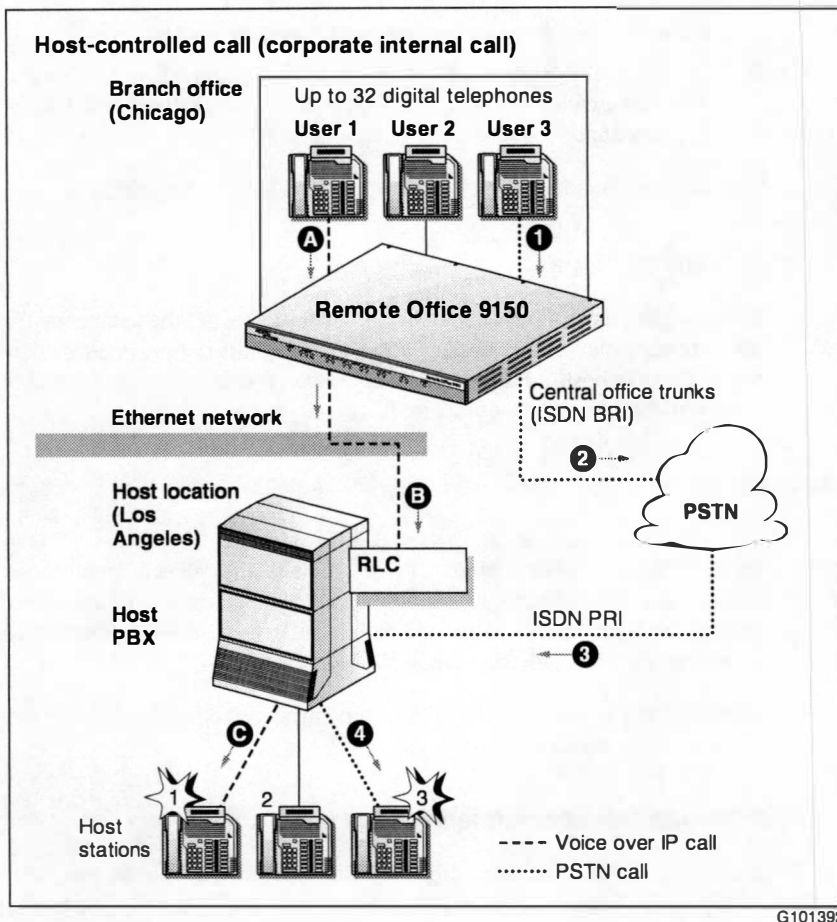
The host PBX is not involved in locally controlled mode calls. See the sample illustration on page 26.

Quality of Service transitioning technology

If the QoS on the IP network falls below a predefined threshold, you can configure the Remote Office 9150 unit to automatically route voice traffic away from the IP network connection to the circuit-switched connection. See "Quality of Service transitioning technology" on page 39 for a detailed description.

Call scenario 1: host-controlled—internal corporate call

The following diagram shows how a call is routed when making a host-controlled call to the corporate office.



The network that is used to route the host-controlled call is transparent to the user, and the dialing requirement is the same for both. Calls work the same way in reverse, from host PBX site to the Remote Office 9150 site.

Voice over IP network call

- 1 User 1 presses the host call appearance key.

Result: User 1 hears a dial tone. This indicates that the connection to the RLC over the IP network was successful.

- 2 User 1 dials a telephone number (such as the extension number of host station 1).

Result: The dialed digits are sent by the Remote Office 9150 unit as packets across the Ethernet network. The RLC converts the packets to the format required by the PBX. The PBX then converts the data to voice and routes the call to host station 1.

PSTN call

- 1 User 3 presses the host call appearance key.

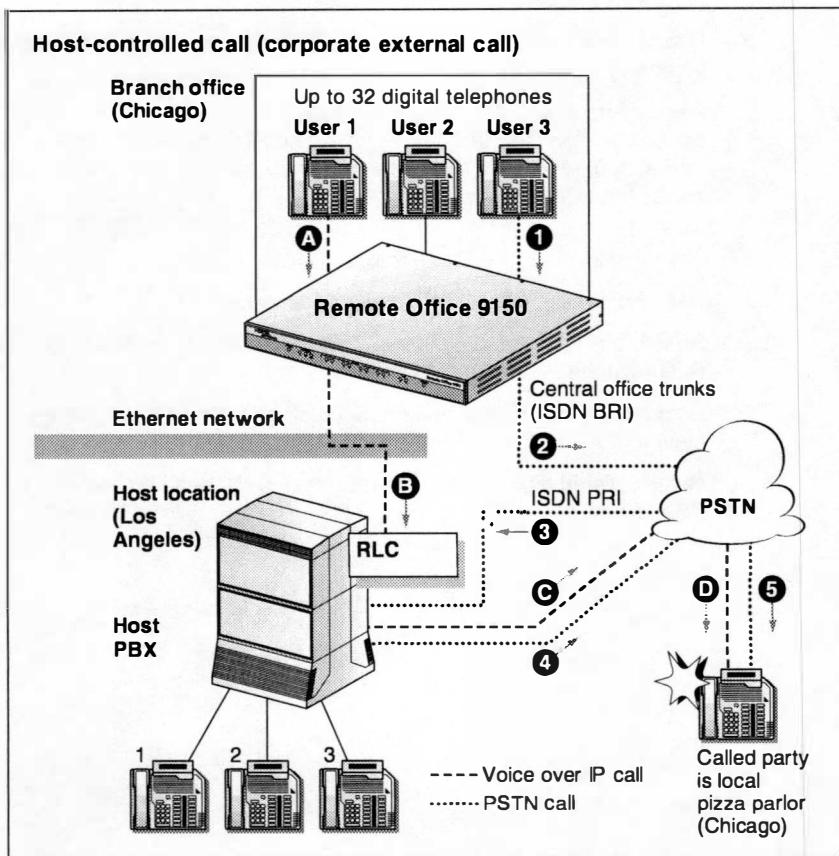
Result: User 3 hears a dial tone. This indicates that the connection to the RLC over the PSTN was successful.

- 2 User 3 dials the telephone number (such as the extension number of host station 3).

Result: Dialed digits are sent across the PSTN then sent through the host PBX to host station 3.

Call scenario 2: host-controlled—external corporate call

The following diagram shows how a call is routed when making a host-controlled call to a party outside the organization.



G101393

The network used to route the call is transparent to the user, and the dialing requirement is the same for both. Calls work the same way in reverse, through the host PBX site to the Remote Office 9150 site.

Voice over IP network call

- 1 User 1 presses the host call appearance key.

Result: User 1 hears a dial tone. This indicates that the connection to the RLC over the IP network was successful.

- 2 User 1 dials the external telephone number.

Result: The dialed digits are sent by the Remote Office 9150 unit as packets across the Ethernet network. The RLC converts the packets to the format required by the PBX. The PBX then converts the data to voice and routes the call through the PSTN to the called party.

PSTN call

- 1 User 3 presses the host call appearance key.

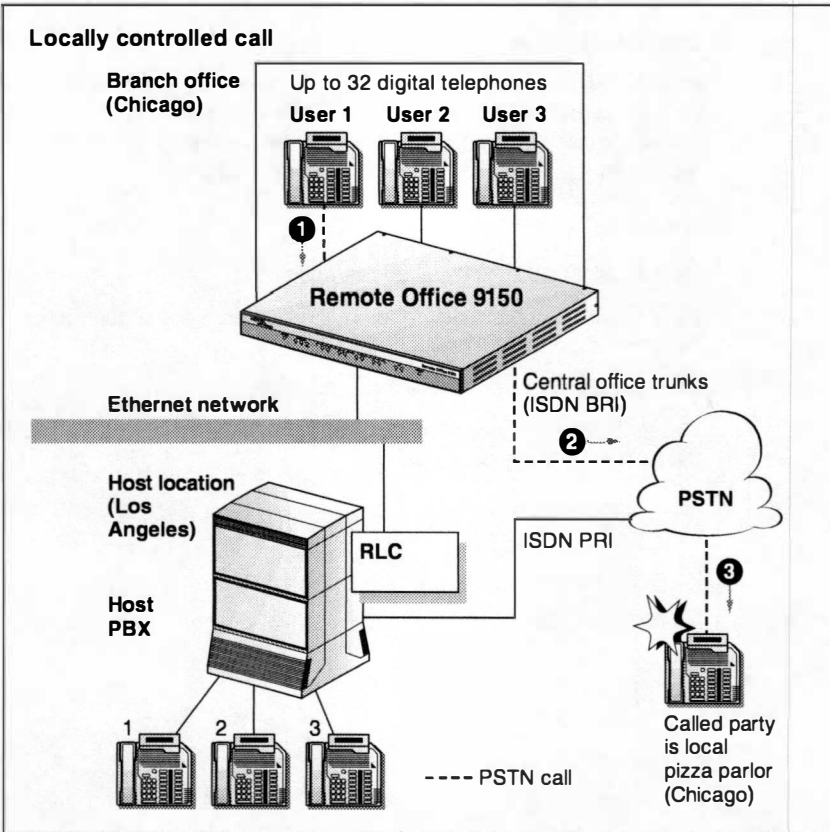
Result: User 3 hears a dial tone. This indicates that the connection to the RLC over the PSTN was successful.

- 2 User 3 dials the external telephone number.

Result: Dialed digits are sent across ISDN BRI through the PSTN, through the host PBX to the called party.

Call scenario 3: locally controlled mode—local call

The following diagram shows how a call is routed when making a call within your local area.



Local call

- 1 User 1 presses the local call appearance key and hears a dial tone from the Remote Office 9150 unit.
- 2 User 1 then dials a trunk access code (such as #61) and hears a dial tone from the Central Office (PSTN).

Note: If all trunks are busy and unavailable, then User 1 hears a fast busy signal.

- 3 User 1 dials the telephone number (the pizza parlor in this example). The dialed digits are sent across the ISDN BRI connection through the PSTN to the called party.

Section B: Features description

In this section

System security	30
Trunking, connection types, and call timers	32
Telephones	35
Voice over IP features	37
Port management	40
Station priority	41
Connection bandwidth	43
Local calling	44
Online/offline table	46
Other supported features	47
Administration software	48

System security

This section describes the security levels that are supported for controlling access from the Remote Office 9150 unit to the RLC on the host PBX.

No security

When no security measures are used, the RLC accepts all incoming calls from the Remote Office 9150 site.

Use this level with caution as it can be prone to unauthorized use. For example, a user in your site could accidentally, or intentionally, enter a trunk number for another site and place long distance phone calls through this connection.

Caller Identification (ID)

When Caller ID is used, and the PSTN routes the call, the RLC identifies the Remote Office 9150 unit's calling line identification (CLID). If the CLID matches the remote number configured on the port assigned to the Remote Office 9150 unit, access is granted. If the incoming call's CLID does not match, access is denied.

Note: Caller ID authentication cannot be performed over the IP network.

Provision ID

You can use Provision Identification (ID) authentication over the IP network or PSTN. When you choose Provision ID, the Remote Office 9150 unit sends its 10-digit security identifier (password) for each connection request. The RLC compares the security identifier with the one configured on the RLC port where the Remote Office 9150 unit is assigned. If the security identifiers match, access is granted.

If the security identifiers do not match then an event is recorded in the Remote Office 9150 unit system log, which can be viewed in Configuration Manager. The telephone that was used to make the call displays a message indicating that communications with the host PBX are down.

You must configure two security identifier passwords on the Remote Office 9150 unit:

- inbound security identifier: This is the RLC's security identifier. It is presented on incoming calls.
- outbound security identifier: This is the Remote Office 9150 unit's security identifier. It is presented to the RLC on outgoing calls.

You must configure the same security identifiers in reverse on the RLC port to which this Remote Office 9150 unit is assigned.

Trunking, connection types, and call timers

This section describes the features that are supported on the PSTN.

Trunk connections

The following digital trunk connections are supported:

- ISDN BRI from the Remote Office 9150 unit to the PSTN
- ISDN PRI from the PSTN to the RLC at the host site

Remote Office supports Multiple Subscriber Numbering (MSN). If the Central Office provides each B-channel with a unique DN then the first B-channel you configure defines the number for both B-channels.

64K (56K) dynamic adaptation

With some carriers, 64K calls routed over a 56K PSTN infrastructure may cause errors. The dynamic adaptation feature allows the Remote Office 9150 unit and the RLC to dynamically detect the limitation of the bandwidth. The call is then downgraded from 64K to 56K.

Bandwidth allocation

The RLC automatically allocates trunk bandwidth to the Remote Office 9150 connection as needed. For example, as calls are initiated and bandwidth requirements increase, additional trunk connections are established. Likewise, as calls terminate and bandwidth requirements drop, connections to idle trunks are terminated.

Connection types

The Remote Office 9150 connection to the RLC can be defined on the RLC as permanent or on demand. A permanent connection means that the ISDN connection to the host PBX always remains open. An on demand connection means that the ISDN connection is established only when a connection with the host PBX is required.

If the connection is defined as demand, then you can configure minimum call duration and idle timers on the RLC to help reduce call charges.

Minimum call duration timer

Most ISDN tariffs specify a minimum length of time for which you are charged when you open the line, regardless of the call duration. This is the same as the minimum call charges listed on long distance telephone bills.

The minimum call duration timer is used in circuit-switched mode only and specifies the minimum length of time that each circuit-switched call to the host PBX remains active, regardless of telephone activity or inactivity. The timer should be configured on the RLC to drop inactive connections just before an additional charge period is incurred. For example, if the timer is set to 59 seconds and your call lasts only 20 seconds, the ISDN connection drops when the timer reaches 59 seconds.

If another call is made to the host PBX before the timer expires, the timer is reset. The timer tracks the current call.

Idle timer

The idle timer identifies the maximum length of time during which an ISDN connection remains idle before it closes. Idle means that a voice connection exists but is not active, and buttons are not being pressed on digital telephones.

For example, if the idle timer is set on the RLC to 60 seconds, the ISDN call remains open for 60 seconds after you hang up. If you or someone else dials another number before 60 seconds have passed, another ISDN connection is not opened.

How the timers work to control ISDN costs

The minimum call duration and idle timers work together to control ISDN charges. The following examples describe what happens when the minimum call duration timer is set to 59 seconds and the idle timer is set to 60 seconds.

Example 1

If the call lasts for 20 seconds and no other calls are made, the ISDN connection drops when the minimum call duration timer reaches 59 seconds. The minimum call duration timer expires before the idle timer.

Example 2

If the call lasts for 65 seconds and no other calls are made, the ISDN connection drops after another 60 seconds has passed without activity. Since the ISDN call exceeded 59 seconds, the minimum call duration timer no longer applies. The idle timer is used, in this case, to prevent further ISDN charges.

Telephones

This section lists the telephones, features, and modules supported by the Remote Office 9150 unit.

Supported digital telephones

The following Meridian digital telephones are supported:

M2008D	M2616CT	M3902
M2008HFD	M3110	M3903
M2216D	M3310	M3904
M2616D	M3820	M3905

Note: The M2006 and M3901 telephones are also supported, but can be used only for locally controlled calls. These telephones do not have displays, which are required for host PBX functionality.

You cannot dial directly from the Call Log of M3900 series telephones because the Trunk Access code and country code may not be displayed.

Supported telephone modules

The following telephone modules are supported:

- add-on modules (to add more keys)
- application modules that provide more functionality
- Meridian Communication Adapters (MCA)
- Analog Telephone Adapters (ATA)

Note: You cannot dial directly from the Call Log of M3900 series telephones because the Trunk Access code and country code may not be displayed.

Computer telephony integration applications

There are two types of computer telephony integration (CTI) applications:

- first-party CTI applications that use the Symposium Desktop TAPI Service Provider
- third-party CTI applications that use Symposium TAPI Service Provider for Meridian 1

Both types can be used with the Remote Office 9150 unit.

TAPI Type	Supported CTI Application
Symposium Desktop TAPI Service Provider 1.6	■ Symposium FastView 1.6 ■ Symposium FastCall 1.6 ■ Symposium Call Manager 5.0 ■ other TAPI-compliant applications
Symposium TAPI Server Provider for Meridian 1 Release 2.1	■ Symposium Agent 1.1 ■ Symposium Call Manager 5.0 ■ other Symposium Partner products

You can use first-party CTI applications with the Remote Office 9150 unit if

- your PC is equipped with a Symposium Communicator card version 1.2 with software version 2.0
- your digital telephone is equipped with a Meridian Communications Adaptor (MCA)

Note: The Symposium Communicator card is not available in all countries. Check with your Nortel Networks distributor for availability.

Automatic Call Distribution (ACD) applications

The Remote Office 9150 unit supports all Nortel Networks ACD applications.

Voice over IP features

You can configure the Remote Office 9150 unit to use the following Voice over IP features:

- Convert analog voice into digital data for transmission as voice packets over the network for calls to or from the fax machine or other analog device that is connected to the analog port on Telco 1.
- Automatically switch from the IP network to the PSTN when the voice QoS falls below a predetermined threshold, and back to the IP network when the QoS returns to normal.

Packetized voice

DSPs located in the Remote Office 9150 unit convert voice into digital data packets and, if compression is used, compresses them. The data is constructed as UDP/IP voice packets for transmission over the IP network.

When voice packets are compressed, they consume less bandwidth, leaving more bandwidth for data or other voice or fax communications. The following algorithms are supported:

- G.711: Packets are transmitted at 64 Kbps (that is, they are not compressed).
- G.726: Packets are compressed and transmitted at 32 Kbps.
- G.729A: Packets are compressed and transmitted at 8 Kbps.

G.729A is the default algorithm on both the RLC and the Remote Office 9150 unit.

In addition to voice compression, the Remote Office 9150 unit supports the following additional packetized voice features:

- A voice jitter attenuation buffer removes the variable delays from the voice packets sent across the IP network, thus avoiding awkward-sounding speech.
- Packet loss handling techniques accommodate missing packets or packets received too late to be processed.

- Silence suppression prevents packet transmission during periods when there is no voice data present. Comfort noise is inserted to assure the user that the line is still active.

Silence is determined when the difference between the adaptable noise floor and the detected signal is less than 9 dB. To prevent clipping, silence must be present for a minimum of 250 milliseconds.

Quality of Service transitioning technology

Communications between the Remote Office 9150 unit in your office and the host PBX take place across the IP network using a 10BaseT Ethernet interface. You can configure the Remote Office 9150 unit to switch automatically from the IP network to the PSTN when the voice QoS falls below a predetermined threshold. Within the QoS settings you can also enable Differentiated Services (DiffServ) and 802.1p mapping to give priority to voice over IP traffic on your network.

Both the RLC and the Remote Office 9150 unit monitor the IP network's QoS constantly. If the IP network QoS degrades, causing poor voice quality, the Remote Office 9150 unit moves, or transitions, the call to the PSTN. When the QoS returns to normal, the Remote Office 9150 unit transitions the call back to the IP network.

For detailed instructions on configuring the thresholds, refer to the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210). For guidelines on evaluating and adjusting the QoS on your IP network, see the *Remote Office Network Engineering Guidelines* (NTP 555-8421-103).

Log reports and statistics

Configuration Manager provides a statistics log that identifies the number of QoS transitions (see "Caller Information Statistics screen" on page 284).

See Chapter 7, "Administration" for a detailed description of log and statistic reports.

Port management

You can assign Remote Office 9150 stations to one of the following types of RLC ports:

- single-user ports
- multi-user voice ports
- dynamic port pool

Port types are assigned on the RLC. Refer to the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210) for detailed instructions.

Single-user ports

Each port that is defined as a single-user (dedicated) port on the RLC supports one Remote Office 9150 station.

Multi-user ports

Ports that are defined on the RLC as multi-user ports allow multiple stations on different Remote Office 9150 units to time-share a single port on the host PBX.

Up to eight persons can share the same RLC port, but not at the same time. All stations that use this type of port must respond to the same DN and have identical phoneset configurations. This port type is especially useful for employees who work mutually exclusive shifts.

Dynamic port pool

Dynamic port pooling is similar to a multi-user port except that the persons who share ports in a dynamic pool are assigned to the next available port in the RLC port pool. There is no correlation between the station and the port on the RLC.

This feature is especially useful in free-seated ACD environments where agents log on to the host PBX using their agent IDs.

Station priority

You can define the priority of a RLC port to which a station is assigned as normal, high, IP only, or circuit only.

Normal priority

When both the IP and PSTN networks are used to route calls, calls to and from the station are routed primarily over the IP network. Calls transition between the IP and PSTN networks whenever voice QoS levels change. (The voice QoS levels are defined on the Quality of Service screen on the RLC for your Remote Office 9150 unit.)

High priority

When you define an RLC port as high priority, the associated station has the following benefits:

- If allowed to use the IP network to process calls (this is transparent to the user), an active call on that station is always one of the first to transition to PSTN trunks when Voice over IP QoS degrades. (This transition is accomplished using the QoS Transitioning Technology.)
- Call blocking is reduced because bandwidth is always available to these stations.

Note: If the reserved bandwidth is being used by other high priority stations, then new calls are processed using unreserved bandwidth.

The number of stations that you can configure as high priority depends on the amount of available bandwidth. Ensure that enough bandwidth is available to process calls on normal priority stations.

IP only

Calls to and from the station are routed over the IP network only. QoS transitioning is not available for stations that are defined as IP only.

Circuit only

Calls to and from the station are routed over the PSTN network only. Circuit only stations never experience voice QoS degradation.

Connection bandwidth

On the connection between the RLC and the Remote Office 9150 unit, you can configure the following:

- when to open additional B-channels (referred to as *extra bandwidth*)
- how much bandwidth to reserve for high priority stations (referred to as *priority reserved bandwidth*)

For instructions, refer to “Configuring ports” in the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210).

Extra bandwidth

When available bandwidth is no longer sufficient to process active calls, additional B-channels are opened according to the extra bandwidth setting. For example, if you configure the extra bandwidth setting as 16 Kbps, another B-channel opens when existing bandwidth is reduced to 16 Kbps or less.

Priority reserved bandwidth

The priority reserved bandwidth setting defines how much bandwidth to reserve for high priority stations. The reserved bandwidth cannot be used by stations configured as normal, IP only, or circuit-only priority. High priority stations consume priority reserved bandwidth before consuming unreserved bandwidth.

For example, if you configure the priority reserved setting as 16 Kbps, then only high priority stations can use this reserved bandwidth. When the reserved bandwidth is being used for active high priority calls, additional calls from high priority stations are processed using unreserved bandwidth. If no bandwidth is available, calls to or from high priority stations are blocked until bandwidth becomes available.

Local calling

The Remote Office 9150 unit allows you to place calls to other extensions within your office or to telephones in your local community. This is accomplished through the use of up to two local call appearance keys. See Chapter 6, "Using Remote Office 9150 stations," for a detailed description of the local call appearance keys.

Local extension calling

When you place a call to another telephone in your office using the local call appearance key, it is handled by the Remote Office 9150 unit, not the host PBX.

Note: If the call is initiated from the host call appearance key, then the station-to-station call requires transmission of signaling data through the host PBX.

Local SwitchOver

Local SwitchOver is a mechanism by which the Remote Office 9150 unit determines that a PBX controlled call that originated on the Remote Office 9150 unit is actually destined for a DN on the same Remote Office unit.

Note: The DN Discovery feature is necessary for the Local SwitchOver feature to work properly. Refer to the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210) for more information.

In this situation, the Remote Office 9150 unit switches to a local 64K channel and cross-connect the voice-paths of the phone without using wide area bandwidth.

There are times, however, when the Remote Office 9150 unit does not know that an incoming and outgoing call are part of the same call (for example, you transfer/forward a call within the same PBX, or redial the last number). Although the call still functions, it consumes Wide Area bandwidth.

Local SwitchOver is not available if the call is answered with the Handsfree button on M39xx telephones.

Local calls through PSTN

The Remote Office 9150 unit allows you to make outgoing and answer incoming PSTN calls over the ISDN BRI connection.

See Chapter 6, "Using Remote Office 9150 stations," for a more detailed description of local calling.

Bridge Port

Bridge Ports are proxy ports that represent local calls or inbound PSTN calls to the PBX. When a local call on a Remote Office 9150 unit needs PBX services, the Bridge Port obtains a PBX presence on behalf of the local call.

Call restrictions

To prevent outgoing calls to certain types of numbers (for example, 1-976), you can disable outgoing calls to specific digit sequences.

Telephone features that are supported

The following Meridian telephone features are supported for locally controlled calls:

- Paging
- Call Waiting
- Hold for calls that appear on local call appearance keys
- Call Transfer (blind and announced) for station-to-station calls only
- Release
- Handsfree
- calling line identification (CLID) and calling party name display (CPND)

Telephone features that are not supported

The Conference and Call Forward features require a host PBX connection, and, therefore are not supported in locally controlled mode.

Online/offline table

The online/offline table is configured on the RLC and allows you to schedule times

- when the ISDN BRI connection to the host PBX is made available to the Remote Office 9150 site

Note: When the Remote Office 9150 unit is in offline mode, users cannot make or receive calls through the host PBX over the IP or PSTN.

- when all telephones at the Remote Office 9150 site revert to normal telephone service

This allows you to ensure that unwanted ISDN BRI telephone calls through the host PBX are disabled after business hours.

How the table works

You can define up to eight entries per day, every day of the week, for each remote site. You can define each entry as online, offline, or undefined for each time period entered.

Users at the Remote Office 9150 site can override the settings of the online/offline table, should the table attempt to suspend access to the host PBX in the middle of a business call. Each user station at the remote site is alerted by a buzz and a display message at 30, 20, and 10 seconds before the connection is terminated. To override connection termination, the user must enter the online SPRE (Special Prefix) code on the telephone.

Configuration

The online/offline table is configured for each remote site on the RLC. Refer to the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210) for configuration information.

For a description of how to go online or offline at the Remote Office 9150 site, see Chapter 6, "Using Remote Office 9150 stations."

Other supported features

Fax support

The Remote Office 9150 unit contains one analog port that can be used to send and receive faxes. You can send and receive faxes in both host- and locally controlled call modes over the IP or PSTN. Faxes are sent uncompressed (that is, you require 64 Kbps of bandwidth).

To support faxing through the host PBX, the fax port on the Remote Office 9150 unit must be associated with a port on the RLC that is configured on the host PBX with voice capability.

Emergency activation code

If your community has implemented an emergency service number (such as 911) to call the police, fire department, or ambulance, you can configure that number on the Remote Office 9150 unit. This allows users in your office to dial the emergency number and be connected directly to the local emergency dispatch center through the PSTN. The call is automatically routed through the local PSTN without having to dial a local trunk access code.

When you configure an emergency activation code on the Remote Office 9150 unit, you also prevent the call from being automatically routed through the host PBX, which could be in a different city. An emergency call that is routed through the host PBX can result in emergency support being dispatched to the wrong location.

ATTENTION

If you are using only the IP network to route calls, you should make emergency service calls on a telephone that is directly connected to a PSTN line. If you make an emergency service call from a station that is connected to the Remote Office 9150 unit, the call is routed through the host PBX, which could be in a different city.

Administration software

Configuration and administration of the Remote Office 9150 unit is performed with Configuration Manager software, a Windows-based application that is installed on your PC.

The software is provided on the Remote Office Product CD-ROM. You can obtain the CD from your Nortel Networks distributor or click on the Customer Support and Software Distribution links at the following website:

www.nortelnetworks.com

Administration PC connection options

You can connect the administration PC to the Remote Office 9150 unit through the following:

- an RS-232 connection to the administration PC's serial port
- a 10BaseT Ethernet interface connection

What you can do with Configuration Manager

Configuration Manager allows you to configure the Remote Office 9150 unit. Configuration Manager also provides the Configuration Wizard for first-time configuration. The Configuration Wizard prompts you for the minimum information that is needed to get the Remote Office 9150 unit communicating with the RLC on the host PBX.

After the initial configuration is completed, use Configuration Manager to administer the Remote Office 9150 unit. Administration tasks include the following:

- viewing the system status
- performing upgrades, backups, or restores
- making configuration changes
- changing the administration password

Note: Configuration Manager alerts you when you must restart after you have made a configuration change.

Command line interface

When the administration PC is connected to the Remote Office 9150 unit through the serial port, you can view the command line interface using an application such as Telnet or HyperTerminal. However, the command line interface is not documented in this guide. Configuration Manager is the supported tool for administering the Remote Office 9150 unit over both the serial port and Ethernet connections.

Chapter 2

Planning for installation

In this chapter

Installation checklist	52
Physical environment	56
Administration PC	61
Network considerations	66
Managing trunk connections	70
Station configuration	73
Security	77
Planning for future growth	79
Deployment options	82
Planning the configuration	87

Remote Office 9150

Installation checklist

Page 1 of 4

Use this checklist to ensure that all installation tasks are completed.

Check	Task	For details, see
☐	Review the <i>Release Notes</i> for last-minute product updates.	<i>Remote Office and RLC Release Notes</i> (NTP 555-8421-102).
☐	Ensure you have the latest firmware and software.	<i>Remote Office and RLC Release Notes</i> (NTP 555-8421-102)
☐	You can route calls over the IP network, the PSTN, or both. Determine, at a high level, what you must do to implement these call routing methods.	"Deployment options" on page 82.
☐	If you want to use the IP network to route calls, evaluate the IP network to determine if the network infrastructure can support voice traffic.	■ your data network administrator ■ <i>Remote Office Network Engineering Guidelines</i> (555-8421-103)
☐	If you want to use the PSTN to route calls, order trunks from the central office to the Remote Office 9150 unit site. Note: The Remote Office 9150 unit supports ISDN BRI trunks (S/T or U interface).	"ISDN BRI information" on page 88.
☐	Obtain the cables that you need to establish the network connections.	"Cables you must supply yourself" on page 59.
☐	Decide on the administration PC setup.	"Administration PC" on page 61.

Remote Office 9150 unit

Installation checklist

Page 2 of 4

Check	Task	For details, see
☐	Gather the configuration information (network addresses, connection numbers, online/offline schedule, QoS thresholds, and so on).	■ “Deployment options” on page 82 ■ Appendix A, “Planning forms”
☐	Install DSP application and trunk interface modules into the Remote Office 9150 unit.	“Installing a trunk interface or DSP application module” on page 100.
☐	Choose a suitable location for the Remote Office 9150 unit.	“Choosing a suitable location” on page 106.
☐	Install the Remote Office 9150 unit in the chosen location.	“Mounting the Remote Office 9150 unit” on page 106.
☐	Connect the Remote Office 9150 unit to the power source, administration PC, and network.	“Connecting the Remote Office 9150 unit” on page 113.
☐	Power up the Remote Office 9150 unit and observe LED behavior. The Status LED remains lit when the power-up cycle completes successfully.	“Powering up the Remote Office 9150 unit” on page 119.
☐	Install the software from the product CD-ROM or the Nortel Networks web site.	“Installing the software” on page 122.
☐	Configure the IP address, subnet mask, and default gateway on the Remote Office 9150 unit.	“Using the Configuration Wizard to perform initial configuration” on page 124.

Remote Office 9150 unit Installation checklist

Page 3 of 4

Check	Task	For details, see
☐	Configure the following items, as required, to create the communication paths between the Remote Office 9150 unit and the RLC: ■ IP network: RLC's IP address ■ PSTN: ■ RLC's telephone number ■ primary trunk ■ security level and, if required, security identifier	■ "Using the Configuration Wizard to perform initial configuration" on page 124 ■ "Configuring the security level" on page 204
☐	Ping the Remote Office 9150 unit and ensure that it is recognized as a device on the network.	"Testing the network connections" on page 138.
☐	Ensure that the Remote Office 9150 unit's connection information is completed on the RLC.	the <i>Reach Line Card Installation and Administration Guide</i> (NTP 555-8421-210).
☐	Configure user stations with appropriate calling permissions and features.	"Defining stations" on page 225.
☐	Configure ports on the RLC.	the <i>Reach Line Card Installation and Administration Guide</i> (NTP 555-8421-210).

Remote Office 9150 unit

Installation checklist

Page 4 of 4

Check	Task	For details, see
☐	Configure network devices ■ so that voice traffic is not constrained or congested ■ to maximize network efficiency for Voice over IP service	■ your data network administrator. ■ <i>Remote Office Network Engineering Guidelines</i> (555-8421-103)
☐ ☐	Ensure that voice calls can be sent or received over the following: ■ IP network ■ PSTN	your data network administrator.
☐ ☐	Ensure that processing of voice and data traffic over the IP network performs as expected. Adjust QoS transitioning settings, if required.	■ your data network administrator ■ your telecom network administrator ■ <i>Remote Office Network Engineering Guidelines</i> (555-8421-103)
☐	Ensure that calls can be made and received on each station.	"Testing the network connections" on page 138.
☐	Plan for administration training and technical support.	■ Chapter 7, "Administration" ■ Chapter 8, "Troubleshooting"

Physical environment

This section provides the space, temperature, cabling, and mounting information you need to know before you install the Remote Office 9150 unit.

Space

Ensure that the Remote Office 9150 unit is installed in a location that is dry and provides plenty of air circulation.

The chosen location should be within cable-length distance from the following:

- the administration PC (if the serial connection is used)
- the Ethernet hub
- trunk and telephone connection interfaces

The Remote Office 9150 unit can be installed up to

- 1230.7 meters (4000 feet) from the digital telephones
- 307.7 meters (1000 feet) from the analog device

It is recommended that you install the Remote Office 9150 unit in the same room where your communications equipment is installed.

Temperature and humidity

The following table describes the temperature and humidity conditions that the Remote Office 9150 unit can withstand without any performance degradation or damage.

Specification	Minimum	Maximum
Normal operation		
Recommended:		
■ Temperature	■ 15°C (59°F)	■ 30°C (86°F)
■ Relative humidity	■ 20%	■ 55% (non-condensing)
Absolute:		
■ Temperature	■ 10°C (50°F)	■ 45°C (113°F)
■ Relative humidity	■ 20%	■ 80% (non-condensing)
Short term (less than 72 hours):	-40°C (-40°F)	70°C (158°F)
Rate of change	Less than 1°C (33.8°F) per 3 minutes	
Storage		
Recommended temperature	-20°C (-4°F)	60°C (140°F)
Relative humidity	5%	95% (non-condensing)
Non-condensing	-40°C (-40°F)	70°C (158°F)
Temperature shock		
In 3 minutes	-40°C (-40°F)	25°C (77°F)
In 3 minutes	70°C (158°F)	25°C (77°F)
Non-condensing	-40°C (-40°F)	70°C (158°F)

Mounting options

You can place the Remote Office 9150 unit on a desk or in a rack, or you can mount it on the wall.

The Remote Office 9150 unit dimensions are

- 42.5 cm (17 in.) wide (without rack-mounting brackets)
- 29.4 cm (11.75 in.) deep
- 4.4 cm (1.75 in.) high

Mounting the Remote Office 9150 unit in a rack

If you want to install the Remote Office 9150 unit in a rack, the rack slot must

- be large enough to provide air circulation to keep the Remote Office 9150 unit cool
- allow you to securely fasten the Remote Office 9150 unit to the rack using the rack-mount brackets

Mounting the Remote Office 9150 unit on the wall

If you want to install the Remote Office 9150 unit on the wall, you can mount it so the cables from the rear panel are directed either right or left. Ensure that the chosen location allows you to easily view the LEDs on the front panel.

ATTENTION

You must complete wall installation using standard telephony installation practices.

Connections

The following connections are made from the rear panel of the Remote Office 9150 unit to the telephone and data networks:

- Two 25-pair connectors (labeled TELCO 1 and TELCO 2) provide tip and ring connections to stations (telephones) and central office trunks (ISDN BRI). These connections provide the interface to the telephone network and the PSTN.

- An RJ-45 connector (labeled ETHERNET) provides a 10BaseT Ethernet connection. This connection provides the ability to pass both voice and data administration traffic over the existing Ethernet network.
- A DB-9 connector (labeled ADMIN) provides an RS-232 serial port connection. You can use this serial port connection to configure a Remote Office 9150 unit that is directly connected to a PC.
- The DB-25 connector (labeled V.35) is for future use.

Cables included with the Remote Office 9150 unit

The Remote Office 9150 unit package includes the following cables:

- power cord and power supply

Notes:

- In North America, the power cord and power supply are included inside the Remote Office 9150 box. In all other regions, the power supply is provided inside the box. However, the power cord for your region is provided outside the box.
- When the North American power cord and power supply are connected together, they are 3.2 meters (10.4 feet) in length.
- If you connect the Remote Office 9150 unit to an uninterruptible power supply then the UPS must have a minimum of 100 Watts available.
- RS-232 serial cable

If the RS-232 cable is not long enough, you can supply your own cable, up to 15.38 meters (50 feet) in length.

Cables you must supply yourself

The cables used to establish the telephone and Ethernet network connections are industry-standard cables. They are not provided in the Remote Office 9150 package. You must obtain them from your local cable supplier.

Telephone network cables

The telephone network cables establish the telephone and trunk connections.

One end of the cable must provide a male 50-pin connector. (This end connects to the Remote Office 9150 unit.)

Ensure that the other end of the cable matches the connectors needed to connect to the telephones or trunks. (For example, if you are using a BIX block to establish the telephone connections, you might need to cut off the connector to expose the wires inside.)

Notes:

- Two telephone cables may be required, based on how many telephones and ISDN BRI lines you plan to connect. (Each telephone cable provides support for up to 16 digital telephones, and two ISDN BRI lines providing two B-channels each. The Telco 1 cable also provides support for one analog station such as a fax machine.)
- The Telco 1 and 2 connections are the opposite gender of the connections for an Meridian 1 IPE or Option 11 cabinet line card slot. Therefore, you must use different cables when connecting to the Remote Office 9150 than those used to connect to Meridian 1 line cards.
- Digital telephones should be located no further than 1230.7 meters (4000 feet) from the Remote Office 9150 unit.
- The analog device should be located no further than 307.7 meters (1000 feet) from the Remote Office 9150 unit.

Ethernet cable

If you are connecting the Remote Office 9150 unit to a hub, you need a standard CAT5 unshielded twisted-pair (UTP) straight-through Ethernet cable. The cable should be no longer than 100 meters (325 feet) in length.

Administration PC

The administration software is Windows-based and is installed on a PC. This section describes ways that you can connect an administration PC to the Remote Office 9150 unit. It also describes the hardware and software requirements for using the administration software.

Connection options

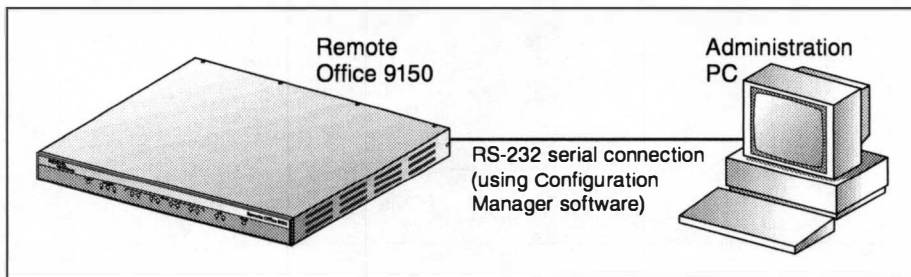
The Remote Office 9150 product includes the Configuration Manager software that enables you to configure, administer, and upgrade the Remote Office 9150 unit. You can perform these tasks over one of the following:

- an RS-232 serial connection (required for first-time configuration only)
- a 10BaseT Ethernet connection (for ongoing administration and upgrades)

Serial connection

You must use the serial connection when you first install and configure the Remote Office 9150 unit. You must establish a serial connection to the Remote Office 9150 unit to enter the IP interface information.

See the following diagram.



G101417

You can continue using the serial connection for ongoing administration of the Remote Office 9150 unit, if you wish. However, if this is the only connection option used, you cannot administer the Remote Office 9150 unit remotely or perform upgrades.

Note: When the administration PC is connected to the Remote Office 9150 unit through the serial port, you can view the command line interface using an application such as Telnet or HyperTerminal. However, the command line interface is not documented in this guide. Configuration Manager is the supported tool for administering the Remote Office 9150 unit over the serial port.

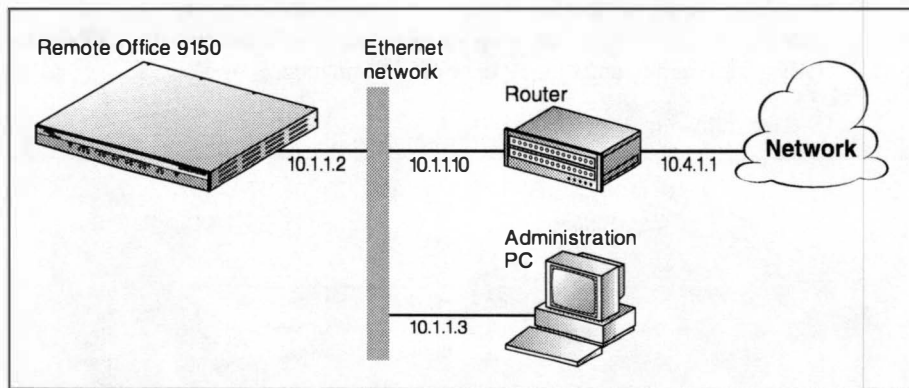
Ethernet connection

Once you configure the Remote Office 9150 unit with its IP interface information, the following can happen:

- Communication can be established between the Remote Office 9150 unit and the RLC (that is, calls can be routed over the IP network).
- You can administer and upgrade the Remote Office 9150 unit over the IP network.

This means you do not have to install an administration PC in the same location as the Remote Office 9150 unit.

See the following diagram.

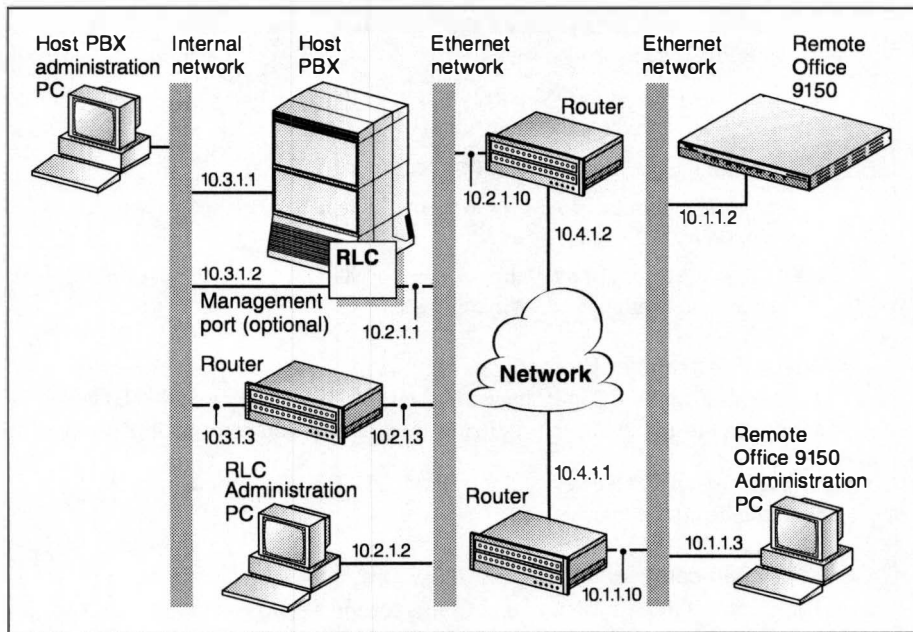


G101415

Administering multiple nodes in the network

If you are responsible for administering one or more Remote Office 9150 units and the RLC on the host PBX, you can access the Remote Office 9150 unit and the RLC from anywhere on the network. The following diagram shows an example of an assembled network with administration PCs.

Note: You do not have to install separate administration PCs for the RLC and the Remote Office 9150 unit. You can use one administration PC to administer all units in the Remote Office network.



G101400

Windows PC requirements

To use Configuration Manager, the administration PC must:

- be an IBM-compatible PC
 - use Windows 95, Windows 98, or Windows NT Workstation (Service Pack 5 or later) with the Microsoft TCP/IP networking component installed
- Note:** Windows 2000 is not supported.
- be equipped with a CD-ROM drive
 - be equipped with a 10BaseT Ethernet interface card (this provides access to the Ethernet network)
 - have an available COM port if you wish to use the RS-232 serial port to establish a direct serial connection
 - be equipped with a pointing device (mouse)
 - have 32 Mbytes of RAM for Windows 95 and 98, or 64 Mbytes of RAM for Windows NT
 - have 48 Mbytes of available storage for Windows 95 and 98, or 64 Mbytes of available storage for Windows NT

Trivial File Transfer Protocol server

The administration PC must have a Trivial File Transfer Protocol (TFTP) server application installed to perform firmware upgrades and configuration uploads.

You can use any TFTP server application. TFTP server applications are available from the Internet.

Year 2000 compliance

The Remote Office 9150 unit and Configuration Manager software are Year 2000 compliant. However, you must ensure that the administration PC is Year 2000 compliant by verifying that the Windows operating system is listed in this table:

Operating system	Year 2000 compliance requirement
Windows NT Workstation	Service Pack 5 or higher
Windows 95	Version 95b

Operating system	Year 2000 compliance requirement
Windows 98	OK as is

Meridian Administration Tools and Configuration Manager

Meridian Administration Tools (MAT) and Configuration Manager are not guaranteed to operate simultaneously on the same administration PC. Simultaneous operation of these two applications on the same PC has not been tested and therefore, is not supported.

Network considerations

The Remote Office 9150 unit communicates through both the IP and telecommunications network using a host PBX.

To use the Remote Office 9150 unit in these networks, you must consider the issues described in this section.

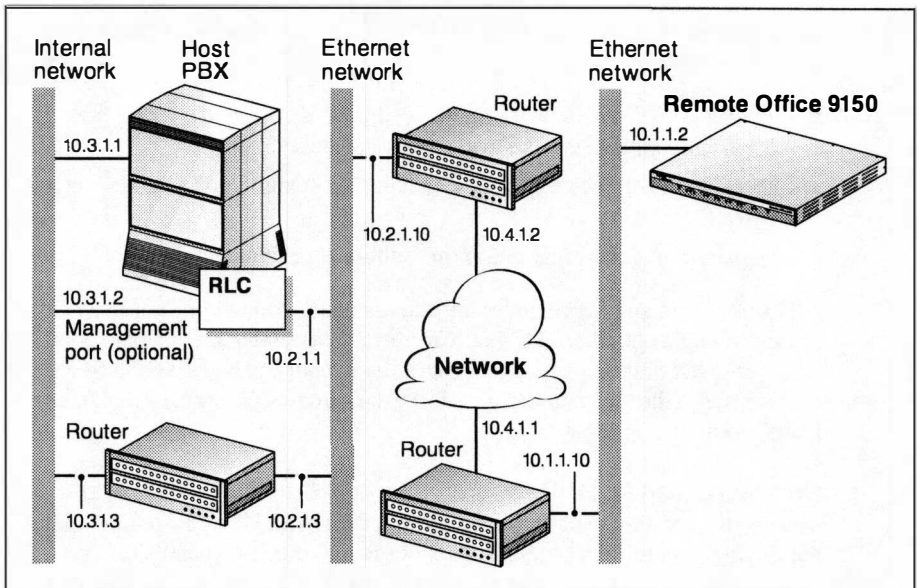
IP addressing and routing

To make and receive calls over the IP network, the Remote Office 9150 unit must be:

- physically connected to the IP network
 - assigned a subnet mask, default gateway, and unique IP address
- Note:** Similarly, a subnet mask, gateway, and unique IP address must be assigned to the RLC on the host PBX.
- able to send and receive traffic to and from the RLC on the host PBX

Network diagram

The following diagram shows the Remote Office 9150 unit's position in an IP network.



G101418

Note: For placement of one or more administration PCs, see “Administration PC” on page 61.

Quality of Service

The routers used on your IP network must be capable of handling voice traffic, with little or no congestion and few delays. If the network is congested or subjected to many delays, voice quality is affected.

For more information, see the *Remote Office Network Engineering Guidelines* (555-8421-103).

Numbering plans

Each trunk groups at the Remote Office 9150 unit site must be assigned a trunk access code (that is, the number dialed to obtain an outgoing trunk). In addition, special prefix (SPRE) codes must be defined for the following features if you want to use them:

- paging
- local calling on ATA-equipped analog devices
- to go online or offline (for more details, see “Online/offline table” on page 46)
- registration and deregistration for multi-user or dynamic ports

All trunk access and SPRE codes are automatically defined in Configuration Manager with a pound prefix (# in North America) so that there are no conflicts with host PBX dialing plans. For a list of the default trunk access and SPRE codes, refer to the “Remote Office 9150 Configuration Information—Dialing Plans” form on page 354.

Numbering plan for local stations

You should consider the numbering plan on the host PBX when setting up the numbering plan for local stations at the Remote Office 9150 unit site. This ensures that station-to-station calls through the host PBX complete correctly.

Call blocking

Call blocking can occur when there are more users installed and more calls being processed than can be supported by the Remote Office 9150 unit’s DSP application and trunk interface modules.

The voice processing capacity of the Remote Office 9150 system depends on the number of DSP application and trunk interface modules installed in the Remote Office 9150 unit and the amount of bandwidth available to process calls. If bandwidth is not available, additional calls are blocked. (This setting is configured on the RLC for each site). This voice processing capacity defines how many calls can be active at one time.

The Remote Office 9150 unit ships with the ability to support up to 32 users, with up to 8 simultaneous calls (providing a 4:1 call blocking ratio). By adding additional DSP application or trunk interface modules, you can reduce or eliminate call blocking.

Reducing call blocking between the Remote Office 9150 unit and the host PBX

Each DSP application module provides the ability to support eight more simultaneous calls when voice traffic is routed over the IP network. Up to three more DSP application modules can be installed in the Remote Office 9150 unit, allowing 32 active calls at one time.

Note: If you add DSP capacity to the Remote Office 9150 unit, you must add the same DSP capacity to the RLC on the host PBX.

Trunks are required for the Remote Office 9150 unit to operate in circuit-switched mode (that is, over the PSTN instead of the IP network). Trunks are used to route calls between the Remote Office 9150 unit and the host PBX or the local PSTN.

By default, the Remote Office 9150 unit ships with no trunks installed. Trunks can be provided by installing trunk interface modules.

The number of trunks you can install depends on the type of trunk interface modules used on the Remote Office 9150 unit. For example, if ISDN BRI trunks are used, each trunk interface module provides one BRI trunk (providing two B-channels). You can install up to four trunk interface modules in the Remote Office 9150 unit.

Note: The Remote Office 9150 unit supports only ISDN BRI S/T or U trunks.

Calculating system requirements

To determine how many DSP application or trunk interface modules are needed to reduce or eliminate call blocking, use the "Remote Office 9150 System expansion worksheet" on page 355.

Managing trunk connections

You can manage trunk connections to the host PBX in several ways:

- Put the Remote Office 9150 unit into offline mode, so that it cannot receive or make calls through the host PBX when operating in circuit-switched mode.
- Define call duration and idle timers, if the trunk connection is defined as on-demand.
- Define minimum and maximum bandwidth allocation settings.
- Use the QoS transitioning technology.

Quality of Service transitioning technology

On IP networks, traffic congestion or delays can occur that result in poor voice quality or lost connections. The RLC can be configured to transition call processing from the IP network to the PSTN when the Quality of Service degrades. When Quality of Service on the IP network returns to normal, call processing can be transitioned back to the IP network.

The points at which the transition occurs are determined by the Quality of Service thresholds (level and duration) defined on each RLC port. To determine appropriate thresholds for each site in your network, you should consult your data network administrator. For more information, see the *Remote Office Network Engineering Guidelines* (555-8421-103).

Online/offline schedule

You can configure an online/offline schedule on the RLC to control when the Remote Office 9150 unit can make and receive calls through the host PBX. When the Remote Office 9150 unit is in offline mode, calls cannot be made or received through the host PBX over the IP or PSTN.

You should configure offline entries:

- for times when the connection to the host PBX should not be active, such as during evenings and weekends
- to prevent the Remote Office 9150 unit from staying online permanently, thereby eliminating unwanted ISDN BRI charges

When the RLC processes an offline entry, it instructs the Remote Office 9150 unit to go offline for a specified number of hours and minutes. The number of hours and minutes the Remote Office 9150 unit stays offline is the difference between the offline entry being processed and the next online entry.

For example, an offline entry is configured at 6:00 p.m. The next online entry is configured at 9:00 a.m. the following day. When the RLC processes the 6:00 p.m. entry, it instructs the Remote Office 9150 unit to go offline for 15 hours.

When going offline, a timer is activated within the Remote Office 9150 unit. When the timer expires (in the example above, at 9:00 a.m.), the Remote Office 9150 unit automatically initiates a “going online” request to the host PBX. If the RLC successfully receives the request, the Remote Office 9150 unit and its connected telephones go online.

Changing the online/offline mode

Whether an online/offline schedule is used or not, you can put the Remote Office 9150 unit into online or offline mode at any time by dialing the online or offline SPRE code at any phoneset connected to the Remote Office 9150 unit. The SPRE codes are configured on the Remote Office 9150 unit.

Trunk bandwidth allocation

The Remote Office 9150 unit can dynamically allocate available trunk bandwidth to active calls in circuit-switched mode. As calls are initiated and bandwidth requirements increase, additional trunk connections are established. Similarly, as calls terminate and bandwidth requirements drop, calls are aggregated and idle trunks are shut down.

Station configuration

When planning the stations at the Remote Office 9150 site, you must think about the call capabilities required by each station.

Each station at the Remote Office 9150 site inherits settings such as voice compression and priority from the RLC port with which it is associated. At the Remote Office 9150 site, the station is configured with the ability to make locally controlled calls, host-controlled calls, or both local- and host-controlled calls. For stations defined with local- or local- and host-controlled capability, specific features can be enabled or disabled.

RLC settings

You must define the following on each RLC port:

- port allocation as dedicated, multi-user, or dynamic
- whether voice compression will be used
- priority level

Port allocation

Assign each user at the Remote Office 9150 site to one port on the RLC on the host PBX. You can configure an RLC port in one of the following ways:

- as a dedicated port (one port per remote user)
- as a multi-user port (one port shared by multiple users)

Up to eight persons can share the same RLC port, but not at the same time. All stations that use this type of port must respond to the same DN and have identical phoneset configurations. This port type is especially useful for employees who are working in mutually exclusive shifts.

- as part of a dynamic pool

Dynamic port pooling is similar to a multi-user port except that the persons who share ports in a dynamic pool are assigned to the next available port in the RLC port pool. There is no correlation between the station and the port on the RLC.

This feature is especially useful in free-seated ACD environments where agents log on to the host PBX using their agent IDs.

Voice compression

If calls are to be routed over the IP network, you must select one of the following voice compression algorithms on each RLC port:

- G.711: Voice is transmitted at 64 Kbps (no compression).
- G.726: Voice is compressed and transmitted at 32 Kbps.
- G.729A: Voice is compressed and transmitted at 8 Kbps.

G.729A is the default voice compression algorithm used by the RLC. This allows

- up to six simultaneous voice calls to be processed over the first ISDN BRI B-channel (16 Kbps are reserved for signaling data)
- up to eight simultaneous voice calls to be processed over the remaining ISDN BRI B-channels

Each Remote Office 9150 station inherits its compression algorithm from the RLC port to which it has been assigned.

Station priority

You can configure each RLC port that is assigned to each station as normal priority, high priority, circuit-switched only, or IP only.

When the port is configured as high priority and the priority reserved setting is configured on the connection between the RLC and Remote Office 9150 unit, you can ensure voice Quality of Service for calls to and from those stations.

For more details, see “Station priority” on page 41 and “Connection bandwidth” on page 43.

Notes:

1. Each Remote Office 9150 station inherits its priority setting from the RLC port to which it has been assigned.
2. The number of RLC ports that you can configure as high priority depends on the amount of available bandwidth. The RLC administrator must ensure that enough bandwidth is available to process calls on normal priority ports.

Remote Office 9150 settings

You can define the following settings for each Remote Office 9150 station:

- port type as local, remote, or both
- extension (directory) number (on local stations only)
- key placement (on local stations only)

Port types

On the Remote Office 9150 unit, you can define each station with one of the following capabilities:

- local control only (local)
You can use stations defined as *local* to make and receive calls through the local PSTN. You can also make station-to-station calls at the Remote Office 9150 site. Calls through the host PBX are not allowed.
- host control only (remote)
If a particular station is not allowed to make or receive calls through the local PSTN, that station is configured as *remote* only. All calls are routed through the host PBX, except for emergency calls (such as 911). If the emergency service number is configured on the Remote Office 9150 unit, calls made to the emergency number are routed through the local PSTN so the emergency service receives the correct location information.
- both local and remote control
You can use stations defined as *local and remote* to make and receive calls through both the host PBX and the local PSTN. You can also make station-to-station calls at the Remote Office 9150 site.

Outgoing calls are routed according to the call appearance key used to initiate the call. Calls initiated on the key defined as the primary or host call appearance key are routed through the host PBX. Calls initiated on the key defined as the local call appearance key are routed through the local PSTN, if a trunk access code was dialed before the telephone number.

When a station is configured with local control capability, further configuration of the station is required to

- enable or disable certain features
- disable outgoing calls or single-digit dialing, if required
- define key placement on the telephone

User extension configuration

Each station is assigned a local directory number (DN). The Remote Office 9150 unit uses the DN to route the incoming call to the correct station.

Stations that are configured with host-controlled call capability are associated with a port number on the RLC. The RLC and the Remote Office 9150 unit use this port number to establish the communication path between the host PBX and the station.

Placement of local call appearance and feature keys

When determining the placement of the local call appearance key on a station, ensure that the key position is not already configured for a specific feature on the host PBX. If you configure a PBX-configured feature key as a local call appearance key, the user cannot use that feature.

If the station is configured with local control capability, you can also configure the placement of other keys, such as Transfer, Call Waiting, and Make Set Busy.

Security

The RLC and Remote Office 9150 unit offer the following types of security:

- security level and, if required, security identifier to prevent toll fraud on the host PBX
- two levels of administration passwords to secure node configurations

Toll fraud

You can minimize toll fraud on the PBX by implementing one of the following levels of security:

- Caller ID

When Caller ID is selected, the Remote Office 9150 unit's calling line identification (CLID) is compared with its PSTN number configured on the RLC port when a connection to the host PBX is attempted. If they match, the connection is established. If they do not match, the host PBX drops the call.

Caller ID authentication cannot be performed over the IP network.

- security identifier

You can use security identifier authentication over the IP or PSTN. If this level is chosen, a security identifier must be configured on both the Remote Office 9150 unit and the RLC port to which the unit is assigned. When a connection between the host PBX and Remote Office 9150 unit is attempted, the security identifiers are compared. If they match, the connection is established. If they do not match, the host PBX drops the call.

Data network security

The Remote Office 9150 solution does not provide for data network security. If security on the data network is an issue, security must be implemented on the data network devices.

System configuration

The RLC and Remote Office 9150 unit configurations are protected by two layers of security:

- administration password

The administration password is required when starting the Configuration Manager software. If the password is not known, the person attempting to use the Configuration Manager cannot log on to any Remote Office node.

Note: A node is any RLC or remote site connected to the RLC.

- node password

The node password is required before the configuration of a particular node can be displayed or modified.

Planning for future growth

The Remote Office 9150 unit can change or grow along with your telecommunication needs. This section describes planning for accommodating those needs.

Adding DSP modules

The Remote Office 9150 unit ships with the ability to support up to 32 stations (which must all be assigned to one RLC). Up to eight simultaneous voice calls can be supported when calls are routed over the IP network.

You can increase the voice processing capability of the Remote Office 9150 unit by installing up to three more DSP modules. Each DSP module adds support for up to eight more simultaneous calls (to a maximum of 32).

To determine how many DSP application modules you need to install, use the "Remote Office 9150 System expansion worksheet" on page 355. For instructions on installing additional DSP modules, see "Installing a trunk interface or DSP application module" on page 100.

Refer to "Configuring DSP resources" on page 235 for configuration information.

Note: When installing additional DSP modules on the Remote Office 9150 unit, you must also increase voice processing capability on the RLC. The number of modules that need to be added on the RLC depend on the requirements of other remote units connecting to the same RLC. If only this Remote Office 9150 unit is connecting to the RLC, then the same number of DSP modules must be installed on both the Remote Office 9150 unit and the RLC. To calculate the RLC's DSP refer to the expansion worksheet in the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210).

Adding trunk interface modules

Initially, the Remote Office 9150 unit ships with no trunks. As connection needs change, you can add up to four ISDN BRI S/T or U trunk interface modules.

To determine how many trunk interface modules you need to install, use the “Remote Office 9150 System expansion worksheet” on page 355. For instructions on installing or replacing existing trunk interface modules, see “Installing a trunk interface or DSP application module” on page 100.

Maximum configurations

The following table identifies the maximum configurations for the Remote Office 9150 solution:

Component	Maximum
RLC connections	1
	Note: You must assign all users at the Remote Office 9150 site to the same RLC.
DSP application modules	3
ISDN BRI modules	4
ISDN BRI lines	4
	Note: Each line is associated with one ISDN BRI module and provides two B-channels.
Trunk groups	10
Digital telephones	32
Analog telephone or fax machine	1
MCAs or ATAs	■ 4 if the Remote Office 9150 unit is connected to a 1-slot RLC (supporting 16 users). ■ 7 if the Remote Office 9150 unit is connected to a 2-slot RLC (supporting 32 users).

Component	Maximum
MCAs or ATAs (continued)	Notes: ■ You can have eight MCAs or ATAs installed if an analog telephone or fax machine is <i>not</i> installed. ■ The total number of digital telephones and ATAs cannot exceed 32.

Deployment options

You can install and configure the RLC on the host PBX and Remote Office 9150 unit to initially use

- only the IP network (Voice over IP)
- only the PSTN (for example, ISDN BRI trunks)
- both networks (which provides the ability to perform QoS transitions)

If you choose not to use both networks initially, this section suggests how you can gradually phase in Voice over IP and QoS transition functionality.

ATTENTION

Even if you plan to route calls over the PSTN only, you must assign an IP address and gateway to the Remote Office 9150 unit and RLC. This allows you to administer both these nodes from an administration PC that is located elsewhere on the network.

Port and station assignment

Regardless of which network you use initially to route calls, you must plan RLC port and user station assignment. For this release, each user at the Remote Office 9150 site must be assigned to one RLC port that is configured on the host PBX with voice capability.

Exception: You must assign the fax machine and stations that use ATAs or MCAs for data transmission to ports that are configured on the host PBX with data capability.

If the PSTN will be used to route calls, one data port on the host PBX must be dedicated to the Remote Office 9150 site to establish the call connections.

Use the following forms to plan port and station assignment:

- “Remote Office 9150 Configuration Information—Stations” on page 346

- “Reach Line Card Connection Information—16 ports” planning form in the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210).
- “Reach Line Card Connection Information—32 ports” planning form in the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210).

To implement circuit-switched mode

In a network using circuit-switched mode only, all incoming and outgoing calls are processed through the PSTN

- to or from the host PBX (host-controlled mode)
- to or from other PSTN customers (locally controlled mode)

To use this scenario, follow these steps:

- 1 Determine how many simultaneous calls you want to process over the PSTN. This will help you determine how many trunk interface modules and DSP application modules to install on the Remote Office 9150 unit.

To do this, complete the “Remote Office 9150 System expansion worksheet” on page 355.

Similarly, you must calculate how many DSP application modules to install on the RLC (if any), using the “Reach Line Card System expansion worksheet” in the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210).

- 2 Arrange for ISDN BRI lines from the PSTN to the Remote Office 9150 site, if they are not already present.
- 3 Install ISDN BRI trunk interface and DSP application modules on the Remote Office 9150 unit, if needed. Up to four ISDN BRI modules and up to three DSP application modules can be installed.

Similarly, install DSP application modules on the RLC, if needed.

Note: The Remote Office 9150 unit does not ship with trunk interface modules or DSP application modules installed. The RLC does not ship with DSP application modules installed.

- 4 Obtain the ISDN BRI information for each line from the Remote Office 9150 site's PSTN service provider. This information must be configured on the Remote Office 9150 unit.

- 5 Identify the telephone number assigned to the B-channel that will be used as the primary trunk connection to the RLC on the host PBX. This telephone number must be configured on the RLC, and is used by the RLC to establish connections with the Remote Office 9150 unit.
- 6 Similarly, obtain the telephone number assigned to the RLC port to which this Remote Office 9150 unit is assigned. This telephone number must be configured on the Remote Office 9150 unit, and is used by the Remote Office 9150 unit to establish connections with the RLC.

To implement Voice over IP mode

In Voice over IP mode, all incoming and outgoing calls are processed across the IP network to or from the host PBX. Calls that are made to external parties through the host PBX are routed to the PSTN using the host PBX's trunks. Both internal and external calls that are made through the host PBX are referred to as host-controlled calls.

Note: You can implement support for local PSTN calls at the Remote Office 9150 site by adding ISDN BRI lines at that site. Local PSTN calls are referred to as locally controlled calls.

To implement Voice over IP mode in host-controlled mode, follow these steps

- 1 Determine how many simultaneous calls you want to process. This will help you determine how many DSP application modules to install on the Remote Office 9150 unit. To do this, complete the "Remote Office 9150 System expansion worksheet" on page 355.

Similarly, you must calculate how many DSP application modules to install on the RLC (if any), using the "Reach Line Card System expansion worksheet" in the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210).

- 2 Install DSP application modules on the Remote Office 9150 unit, if needed. Up to three DSP application modules can be installed.

Similarly, install DSP application modules on the RLC, if needed.

- 3 Obtain an IP address assigned for the Remote Office 9150 unit. This IP address must be configured on the RLC, and is used by the RLC to establish connections with the Remote Office 9150 unit.

- 4 Similarly, obtain the IP address assigned to the RLC. This IP address must be configured on the Remote Office 9150 unit, and is used by the Remote Office 9150 unit to establish connections with the RLC.
- 5 If IP mode is stage 2 in your network implementation, run this stage with a minimal number of users until you are sure that
 - your IP network can handle the additional traffic
 - you can identify the kinds of configuration adjustments you need to make to the IP network to handle that traffic
- 6 When you are satisfied with the IP network performance, continue with implementing the QoS transitioning technology.

To implement a Remote Office 9150 unit behind a NAT router

Some network routers run the Network Address Translation protocol to allow multiple devices in an Ethernet network to share the same broadband Ethernet address. An alternative to running the NAT protocol is to have the network administrator provide each device with its own broadband Ethernet address. Remote Office 9150 units support NAT functionality. Only a single Remote Office 9150 unit may be connected behind a NAT router. Multiple Remote Office 9150 units may be connected behind a PNAT router. A PNAT router is a port number and network address translation router.

For a Remote Office 9150 unit connected behind a NAT router you must:

- configure a permanent IP signaling connection
- assign a static IP address

Refer to “Configuring the RLC connection information” on page 198 for the procedure.

To implement the Quality of Service transitioning technology

When the QoS transitioning technology is implemented, calls transition

- to the PSTN when IP QoS degrades
- back to the IP network when IP QoS returns to normal

- 1 To implement the QoS transition technology, you must understand what your IP network is doing, such as
 - when the busy times are on the network
 - how much traffic is processed (during normal and busy traffic periods)
 - how to evaluate and adjust your network's Quality of Service

For more details, consult with your data network administrator and refer to the *Remote Office Network Engineering Guidelines* (555-8421-103).

- 2 Once you have this information and understand it, determine what the QoS settings should be, and then configure them on each RLC port.

For instructions, refer to the Reach Line Card Installation and Administration Guide (NTP 555-8421-210).

- 3 If IP mode is the last stage in your network implementation, run this stage with a minimal number of users until you are sure that your IP network's Quality of Service is acceptable.
- 4 When you are satisfied with QoS transition performance, deploy the QoS transition capability to the rest of the network.

Planning the configuration

Before you configure the Remote Office 9150 unit, it is strongly recommended that you complete the data entry forms shown in Appendix A, "Planning forms."

This section describes the information you can configure on the Remote Office 9150 unit.

Data entry form completion sequence

You should complete the data entry forms in the following sequence:

1. Remote Office 9150 Configuration Information—Stations form
2. Remote Office 9150 Configuration Information—ISDN BRI Modules form
3. Remote Office 9150 Configuration Information—Network Connections form
4. Remote Office 9150 Configuration Information—Dialing Plans form

For more details, see Appendix A, "Planning forms."

Station assignments and configuration

You must assign each telephone in your office to one of the 32 ports provided by the Remote Office 9150 unit. You can configure stations with the ability to make locally controlled calls (local), host-controlled calls (remote), or both (local and remote).

If a station will be configured with the ability to make host-controlled calls, then that station is mapped to a RLC port (which, in turn, is mapped to telephone port configuration on the host PBX).

If a station will be configured with the ability to make locally controlled calls (including station-to-station dialing), you must take the numbering plan on the host PBX into consideration. You need to ensure that when users dial another station in the same office in host-controlled mode, the call routes correctly.

Stations that will be used for locally controlled calls can be further configured with features and their key locations.

ISDN BRI information

Providing information to your service provider

To ensure that you get the correct ISDN service for the Remote Office 9150 unit, tell your service provider how the ISDN line should be provisioned. Request the following:

- two B-channels providing voice and data capability
Both B-channels must be Circuit Switched Voice and Data.
- Calling Line Identification (CLI) or Caller ID
CLI provides the caller's telephone number when you receive a call. This information is provided by the network and not the caller, so it can be used as a security measure to identify calls to be accepted and rejected.
- 64 Kbps clear channel
Note: A 64 Kbps clear channel is also required on the ISDN PRI connection between the host PBX and the PSTN. A 56 Kbps channel does not provide enough bandwidth to process one call using G.711 compression.

Receiving information from your service provider

In return for providing the ordering information, your service provider gives you directory numbers and, if used in your area, Service Profile Identifiers (SPIDs). SPIDs are not provided for the AT&T 5ESS Custom service.

A directory number is the address or ISDN telephone number for the ISDN line assigned by the service provider. Each ISDN line receives at least one telephone number, called the Primary Directory Number.

If used in your area, your service provider provides you with the SPIDs. These are associated with the service you have ordered, and you must use these as part of the configuration for the Remote Office 9150 unit before any ISDN connections can be made (except for AT&T Custom). The SPID is similar to the ISDN telephone number and its format is unimportant as long as the information is entered correctly when configuring the Remote Office 9150 unit.

IP addresses

If you want to administer the Remote Office 9150 unit over the IP network, the following information is required for the Remote Office 9150 unit:

- IP address (it must be unique)
- subnet mask
- default gateway

If you want to route voice traffic over the IP network, you also need the RLC's IP address. The Remote Office 9150 unit uses these IP addresses to establish the connection with each other.

Connection between the RLC and Remote Office 9150 unit information

If you want to route voice traffic over the PSTN, the telephone numbers for each end of the network are required. If security is being implemented, the security authentication information (Caller ID or security identifier) is also needed.

Online/offline schedule

You can configure each port on the RLC with a schedule that identifies when a remote site is online (connected to the corporate PBX) or offline. When the Remote Office 9150 unit is in offline mode, calls cannot be made or received through the host PBX over the IP or PSTN.

You can configure only one online/offline schedule for the RLC port. This schedule affects all stations at the Remote Office 9150 site. You should create offline entries

- for times when the connection to the host PBX should not be active, such as during evenings and weekends
- to prevent the Remote Office 9150 unit from staying online permanently, thereby eliminating unwanted ISDN BRI charges

To help you plan the online/offline schedule configuration on the RLC, use the "Reach Line Card Online/Offline Table Configuration" form in the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210).

Trunk configuration information

Trunk configuration on the Remote Office 9150 unit consists of defining the ISDN BRI lines from the central office and assigning one or more B-channels, if desired, to trunk groups.

Numbering plan

You must assign a trunk access code to each trunk group at the Remote Office 9150 unit site. A trunk access code is the number that must be dialed to obtain an outgoing trunk. In addition, you must define special prefix (SPRE) codes for the following features if you want to use them:

- **paging**
- **to go online or offline** (for more details, see “Online/offline table” on page 46)
- **local calling**
This allows analog or ATA-equipped station users to change the outgoing call mode to locally controlled mode. (Host-controlled mode is the default mode when users go offhook on analog or ATA-equipped stations.)
- **registration and deregistration**
The registration SPRE code is used to register the station user with a multi-user or dynamic port.
The deregistration SPRE code disengages the user from the port so that another user can use it. The user is put into *not logged in* mode.

All trunk access and SPRE codes are automatically defined in Configuration Manager with a pound sign (# in North America) so that there are no conflicts with host PBX dialing plans. The maximum length of each code is three digits in addition to the pound sign. For a list of the default SPRE and trunk access codes, refer to the “Remote Office 9150 Configuration Information—Dialing Plans” form on page 354.

Note: You can change the defaults if you wish.

Chapter 3

Installing the Remote Office 9150 unit

In this chapter

General safety	92
Required tools	94
Unpacking and inspecting the equipment	95
Removing the Remote Office 9150 unit cover	97
Installing a trunk interface or DSP application module	100
Mounting the Remote Office 9150 unit	106
Connecting the Remote Office 9150 unit	113
Powering up the Remote Office 9150 unit	119
Installing the software	122
Using the Configuration Wizard to perform initial configuration	124
Testing the network connections	138

General safety

This section describes the general safety guidelines recommended by Nortel Networks. You must follow these safety guidelines whenever you perform installation or maintenance tasks on the Remote Office 9150 unit.

Precautionary messages

This guide provides warnings when risks related to hardware installation and handling are known. For a description of the types of warnings this guide provides, see “Conventions used in this guide” on page xix. Do not ignore these warnings.

Safety precautions

To avoid damage or injury, follow these safety precautions at all times.

Plug the Remote Office 9150 unit into a properly grounded power source to reduce the possibility of electric shock and damage to the unit or network.



DANGER

Risk of electric shock

Disconnect the power as well as the Telco 1 and Telco 2 cables before you perform any hardware troubleshooting or add ISDN BRI or DSP application modules to the Remote Office 9150 unit.

If you do not disconnect the Telco 1 and Telco 2 cables from the Remote Office 9150 unit, you can receive a lethal shock if an external telco line is accidentally severed.

Ensure that nothing rests on connection cables, and that cables cannot be tripped over or stepped on.

Electrostatic discharge safety precautions

Electrostatic discharge (ESD) affects the performance and decreases the useful life of system components. ESD can seriously damage component parts, such as circuit cards.

Implement the following precautions, which are recommended by computer and telephone equipment manufacturers:

- Remove items that generate static charge from the installation site.
- Use antistatic spray if the site is carpeted.
- Ground yourself before handling any equipment. (For example, wear an antistatic wrist strap attached to any unpainted metal surface that is connected to an electrical ground.)

Required tools

This section identifies the tools you need to perform Remote Office 9150 unit installation and maintenance tasks.

Hardware installation tools

You need the following tools to install the Remote Office 9150 unit, or to install or replace DSP application or trunk interface modules:

- an antistatic ESD wrist strap (recommended)
- a Phillips (cross-head) screwdriver
- a pen or pencil for
 - noting the installation location (if mounting on a wall)
 - noting cable lengths
 - labeling cables
- cable tie wraps
- cable identification labels
- a tape measure
- four wood screws if you want to mount the Remote Office 9150 unit on the wall

Software installation or upgrade tools

In addition, if you are performing a first-time installation or a maintenance upgrade, you need the following items:

- the *Remote Office Product CD-ROM*
- a PC with a CD-ROM drive or an Internet connection for obtaining software, firmware, and documentation updates
- a TFTP server application installed on the PC

The TFTP server is required for performing firmware upgrades. If a TFTP server is currently not installed, you can obtain one from the Internet.

Unpacking and inspecting the equipment

Before you install the Remote Office 9150 unit, ensure that the package contents are all present and are not damaged.

Before you begin

Before you unpack the equipment, ensure that your work area is safe from electrostatic discharge. For more details, see “Electrostatic discharge safety precautions” on page 93.

To inspect the package contents

- 1 Inspect the box in which the Remote Office 9150 unit was shipped for damage.
- 2 Open the box and remove its contents.
- 3 Verify that, in addition to this guide, the following items are present:

Check	Item
-------	------

- | | |
|--------------------------|---|
| ☐ | Remote Office 9150 unit |
| ☐ | Package containing rubber feet and rack-mounting brackets with screws |
| ☐ | Power cord and power supply |

Note: In North America, the power cord and power supply are included inside the Remote Office 9150 box. In all other regions, the power supply is provided inside the box and the power cord for your region is provided outside the box.

- | | |
|--------------------------|---------------------|
| ☐ | RS-232 serial cable |
|--------------------------|---------------------|

Check Item

- ☐ Remote Office and RLC Release Notes (NTP 555-8421-102)
 - ☐ Remote Office Product CD-ROM
-

- 4 Visually inspect each item for obvious faults or damage.

What to do if damage is found

If any component is damaged, report the damage immediately to your Nortel Networks distributor and the carrier who delivered the equipment.

What's next?

When you have verified that all components are present and are undamaged, do the following:

- Install DSP application and trunk interface modules, if required.
For instructions, see "Installing a trunk interface or DSP application module" on page 100.
- Install the Remote Office 9150 unit in its chosen location.
For instructions, see "Mounting the Remote Office 9150 unit" on page 106.

Removing the Remote Office 9150 unit cover

As you increase or change the voice processing capability of the Remote Office 9150 unit, you need to perform one or more of the following tasks:

- Install additional trunk interface modules.
- Install additional DSP application modules.

To perform these tasks, you must remove the Remote Office 9150 unit cover.

To remove the Remote Office 9150 unit cover



DANGER

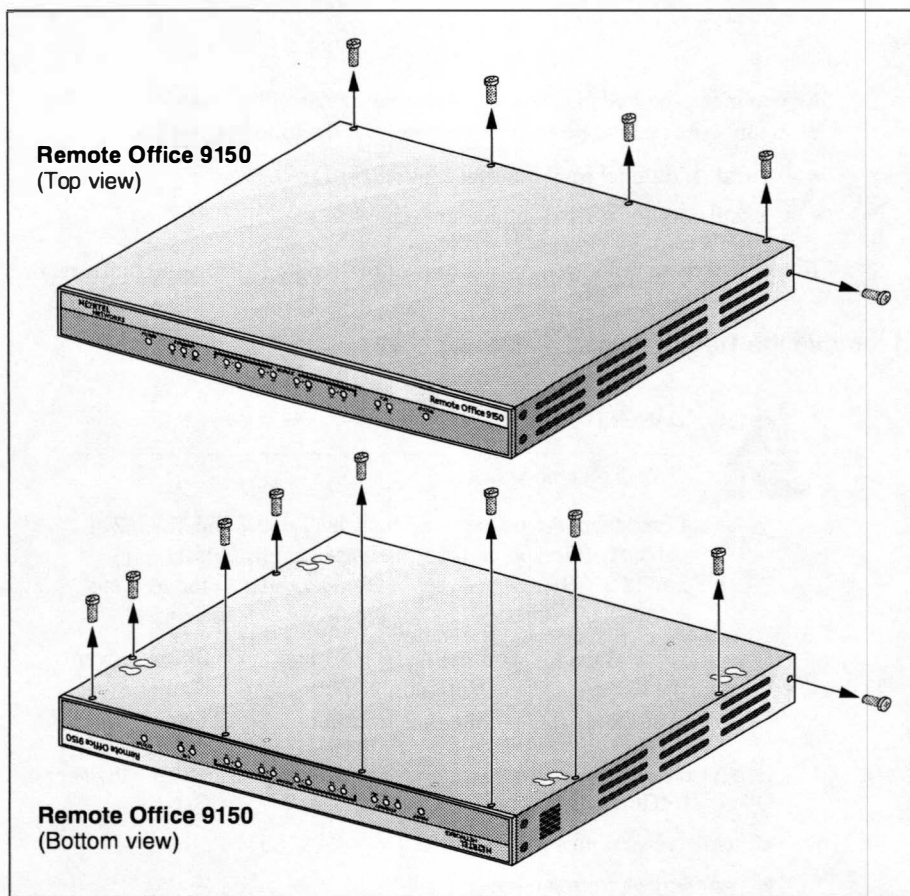
Risk of electric shock

Disconnect the power as well as the Telco 1 and Telco 2 cables before you perform any hardware troubleshooting or add ISDN BRI or DSP application modules to the Remote Office 9150 unit.

If you do not disconnect the Telco 1 and Telco 2 cables from the Remote Office 9150 unit, you can receive a lethal shock if an external telco line is accidentally severed.

- 1 Use a Phillips screwdriver to remove the following screws from the Remote Office 9150 unit cover:
 - two screws from the sides
 - four screws from the top
 - eight screws from the bottom

See the diagram on page 98.



G101406

- 2 Place the screws in a safe place where they cannot be lost.
- 3 Ensure the Remote Office 9150 unit is placed top side up.
- 4 Remove the cover as follows:
 - a. Grasp both sides of the Remote Office 9150 unit.
 - b. Slide the cover toward you.
 - c. Lift the cover off the unit.
 - d. Put the cover aside.
- 5 Turn the Remote Office 9150 unit so the rear panel faces you.
- 6 This allows you to read the labels on the Remote Office 9150 unit circuit board.
- 7 Perform module installation as required.

For instructions, see "To install a trunk interface or DSP application module" on page 103.
- 8 Replace the cover as described in "To replace the Remote Office 9150 unit cover" below.

To replace the Remote Office 9150 unit cover

- 1 Carefully slide the top cover into position over the circuit board so that the holes along the top edge of the rear panel are aligned.
- 2 Replace the four screws on the top.
- 3 Replace the two screws on the sides.
- 4 Turn the Remote Office 9150 unit over and replace the eight screws on the bottom.
- 5 Continue with "Mounting the Remote Office 9150 unit" on page 106.

Installing a trunk interface or DSP application module

The Remote Office 9150 unit ships from Nortel Networks with

- no trunk interface modules installed
- one Digital Signal Processor (DSP) built into the Remote Office 9150 unit's motherboard

What trunk interface modules do

Trunk interface modules route calls over the PSTN. The number of modules you must install depends on the number of simultaneous calls you want to process in host-controlled or locally controlled mode.

Note: To determine how many trunk interface modules you need for your calling requirements, use the "Remote Office 9150 System expansion worksheet" on page 355.

What DSP application modules do

DSP application modules convert voice and fax into digital data for transport over the IP and PSTN.

Initially, the Remote Office 9150 unit ships with the ability to support up to eight simultaneous calls through a DSP that is built into the Remote Office 9150 unit's motherboard. To add support for up to 32 simultaneous calls, you must install DSP application modules. Up to three DSP application modules are supported. Each module provides up to eight more simultaneous calls.

Note: To determine how many DSP application modules you need for your calling requirements, use the "Remote Office 9150 System expansion worksheet" on page 355.

When to install trunk interface or DSP application modules

Perform the procedures in this section when you

- need to expand the Remote Office 9150 unit's voice processing capability and have ordered additional modules (up to four trunk interface modules or three DSP application modules)
- need to replace a module because it is faulty

Before you begin

Before you can install a trunk interface or DSP application module, you must remove the cover from the Remote Office 9150 unit. For instructions, see "Removing the Remote Office 9150 unit cover" on page 97.

ATTENTION

DSP application and trunk interface modules are sensitive pieces of electronic equipment and must be handled as such. Ensure that you follow the electrostatic discharge safety precautions described on page 93.

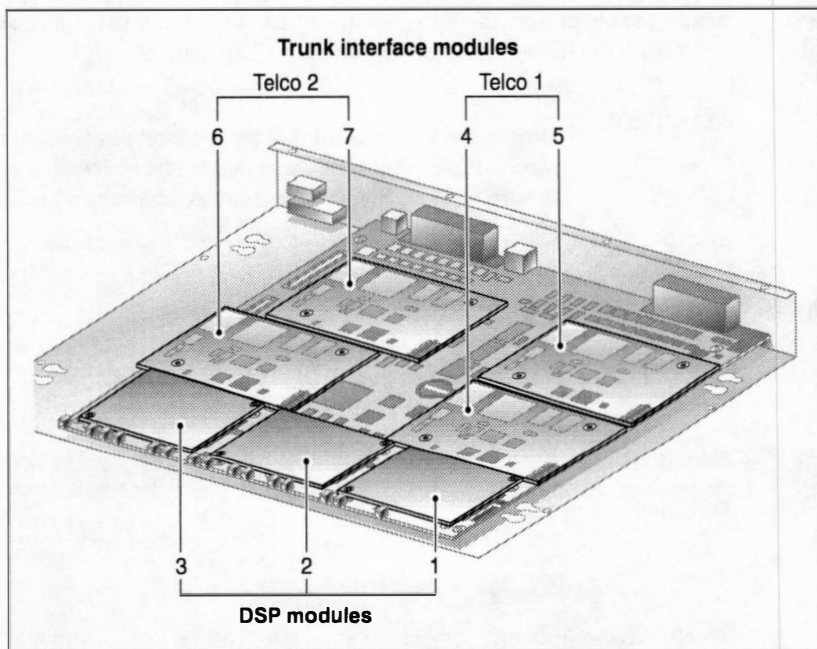
Where the modules can be installed

Each module position is labeled on the Remote Office 9150 unit circuit board as shown in the following table:

Module type	Valid module positions
DSP application module	■ MOD 1 ■ MOD 2 ■ MOD 3
Trunk interface module	Telco 1 connector (phone lines 1 through 16): ■ MOD 4 ■ MOD 5

Module type	Valid module positions
Trunk interface module (continued)	Telco 2 connector (phone lines 17 through 32): ■ MOD 6 ■ MOD 7 Note: Each Telco connector provides access to two ISDN BRI lines (each with two B-channels).

The following diagram shows where you can install the trunk interface and DSP application modules on the Remote Office 9150 unit circuit board:



G101408

Nortel Networks recommends that you populate each module position in sequential order. Install trunk interface modules according to the Telco 1 or Telco 2 connections used.

Note: The Remote Office 9150 unit contains a dongle socket located in the middle of the circuit board. This dongle is not being used.

To remove a trunk interface or DSP application module

Note: Perform this procedure only if you need to replace a trunk interface or DSP application module.

- 1 Use one hand to firmly grasp the long sides of the module that you want to remove.
- 2 Gently lift one side of the module up until it is free of the connectors on the Remote Office 9150 unit circuit board.
- 3 Lift the module up and away from the Remote Office 9150 unit circuit board, and place it to one side.

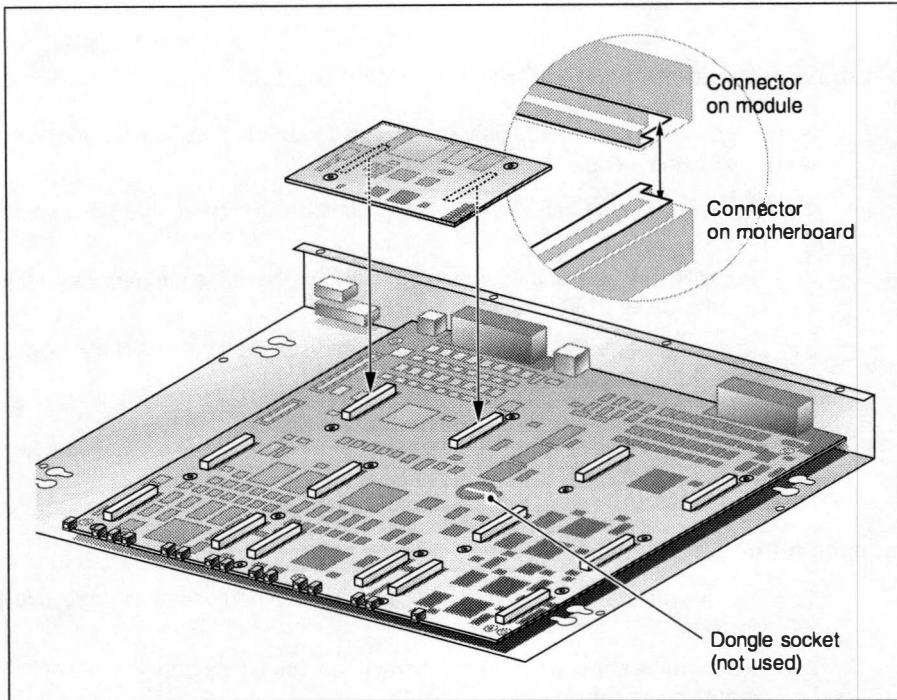
Note: If you are replacing this module, put it inside the replacement module's protective wrapper for storage or return it to Nortel Networks for repair.

To install a trunk interface or DSP application module

- 1 Remove the trunk interface or DSP application module from its protective wrapper.
- 2 Compare the connectors on the module with the connectors in the location where you want to install the module.

The connectors are keyed so that you can install the module in one way only. Ensure you hold the module so that the orientation of the connector keys match.

See "Where the modules can be installed" on page 101, and the diagram on page 104.



G101404

- 3 Align the connectors on the module with the connectors on the Remote Office 9150 unit circuit board.
- 4 Use both hands to grasp the module firmly and push down until it snaps into place.
- 5 Visually inspect the module connectors to ensure there is no gap between the module connectors and the Remote Office 9150 motherboard connectors.
- 6 Ensure the module is securely installed by placing one finger beneath the module and tugging upward. The module should not move.

What's next?

After you have installed the trunk interface or DSP application modules, replace the Remote Office 9150 unit cover, and then install the unit in its chosen location. For instructions, see the following:

- “To replace the Remote Office 9150 unit cover” on page 99
- “Mounting the Remote Office 9150 unit” on page 106

Module configuration

To associate the ISDN BRI line from your ISDN service provider with a particular trunk interface module, you must configure the trunk interface modules in Configuration Manager.

If you have installed one or more modules as part of your first-time installation, complete the remaining procedures in this chapter. Then, complete configuration as required and described in “Configuring BRI trunks” on page 211.

Mounting the Remote Office 9150 unit

The Remote Office 9150 unit can be installed

- on a desk (see below)
- on a wall (see page 108)
- in a rack (see page 110)

The Remote Office 9150 unit package contains the following hardware:

- rubber feet for installing the Remote Office 9150 unit on a desk
- brackets with screws for installing the Remote Office 9150 unit in a rack

If you want to mount the Remote Office 9150 unit on a wall, you must provide your own mounting hardware.

Choosing a suitable location

The Remote Office 9150 unit dimensions are

- 42.5 cm (17 in.) wide (without rack-mounting brackets)
- 29.4 cm (11.75 in.) deep
- 4.4 cm (1.75 in.) high

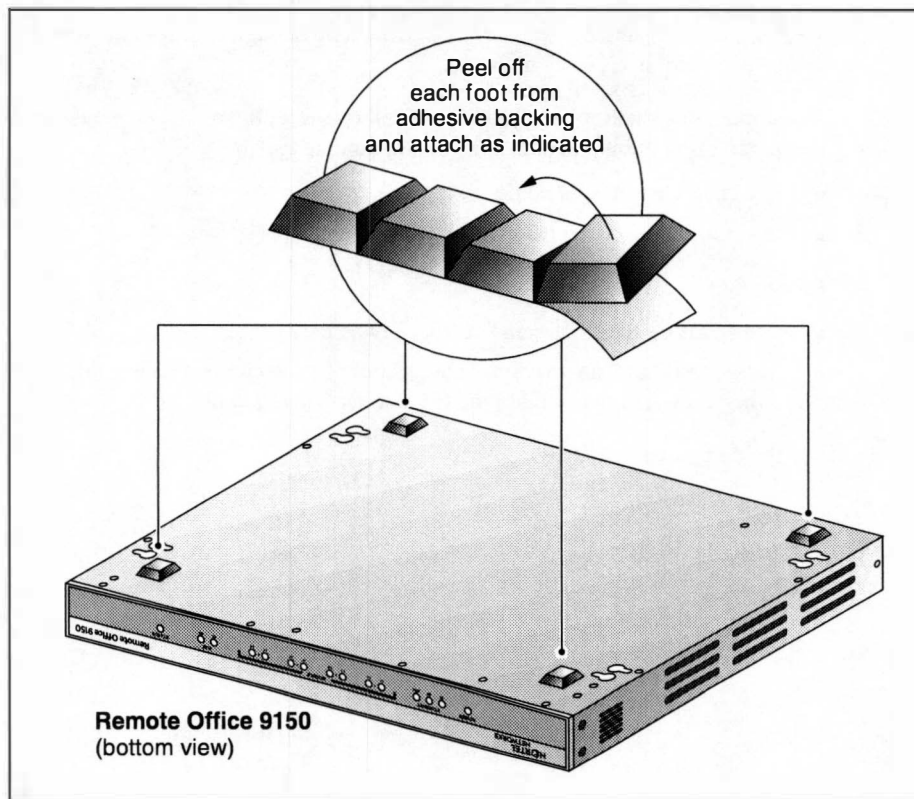
For guidelines on where to install the Remote Office 9150 unit, see “Physical environment” on page 56.

Note: It is recommended that you install the Remote Office 9150 unit in the same room where your communications equipment is installed. The Remote Office 9150 unit should be located no further than

- 1230.7 m (4000 ft) from the digital telephones
- 307.7 m (1000 ft) from the analog device

To install the Remote Office 9150 unit on a desk

- 1 Turn the Remote Office 9150 unit bottom side up.
- 2 Affix the rubber feet to the Remote Office 9150 unit as shown in the following diagram:



G101395

- 3 Ensure the rubber feet are securely fastened.
- 4 Place the Remote Office 9150 unit in the desired location.
- 5 Continue with "Connecting the Remote Office 9150 unit" on page 113.

To install the Remote Office 9150 unit on the wall

Do not affix the rubber feet to the bottom of the Remote Office 9150 unit. Otherwise, the unit cannot be mounted flush against the wall.

To mount the Remote Office 9150 unit on the wall, you must provide your own screws. You need suitable size screws that are long enough to ensure the Remote Office 9150 unit is securely mounted.

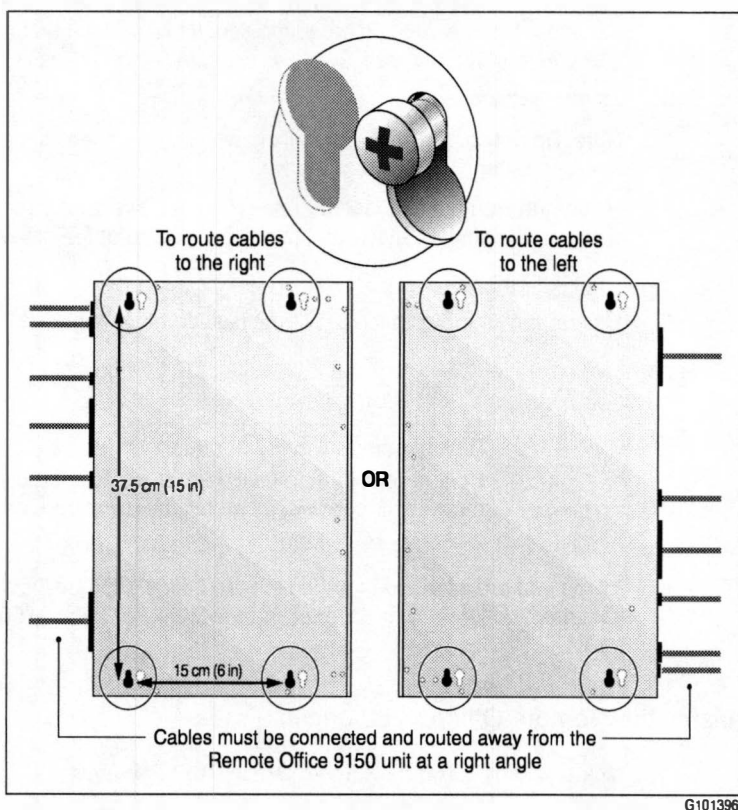
When mounting the Remote Office 9150 unit on the wall, you must use standard telephony installation practices. The unit is mounted so that

- the cables are at right angles to the unit
- the rear (connection) panel faces left or right

Ensure that

- the LEDs on the front panel can be viewed easily
- the chosen location provides enough space to accommodate the cables when they are connected to the Remote Office 9150 unit

See the diagram on page 109.



- 1 Choose the location on the wall where you want to mount the Remote Office 9150 unit.
- 2 Use the predrilled screw slots on the bottom of the Remote Office 9150 unit as a guide to measure and mark the location on the wall for each mounting screw.

The measurements between the screw slots are as follows:

- from front to back panels: 15 cm (6 in.)
- from side to side: 37.5 cm (15 in.)

Note: Two sets of screw slots are provided. Each set allows you to route the cables to the left or right when the Remote Office 9150 unit is correctly mounted. Ensure you use the same screw slot orientation for each location that you mark on the wall.

- 3 Mount the screws.

Note: Do not screw the screws all the way in. The heads should be screwed to about 5 mm (1/8 in.) from the wall.

- 4 Mount the Remote Office 9150 unit on the screws, and then gently pull it down so the screws slide into the narrow portion of the screw slots.

Do not let go yet!

- 5 Ensure the Remote Office 9150 unit is securely mounted.



WARNING

Risk of personal injury or equipment damage

Ensure the Remote Office 9150 unit is securely fastened to the wall. Otherwise, it can fall, be damaged, and cause injury to yourself or others.

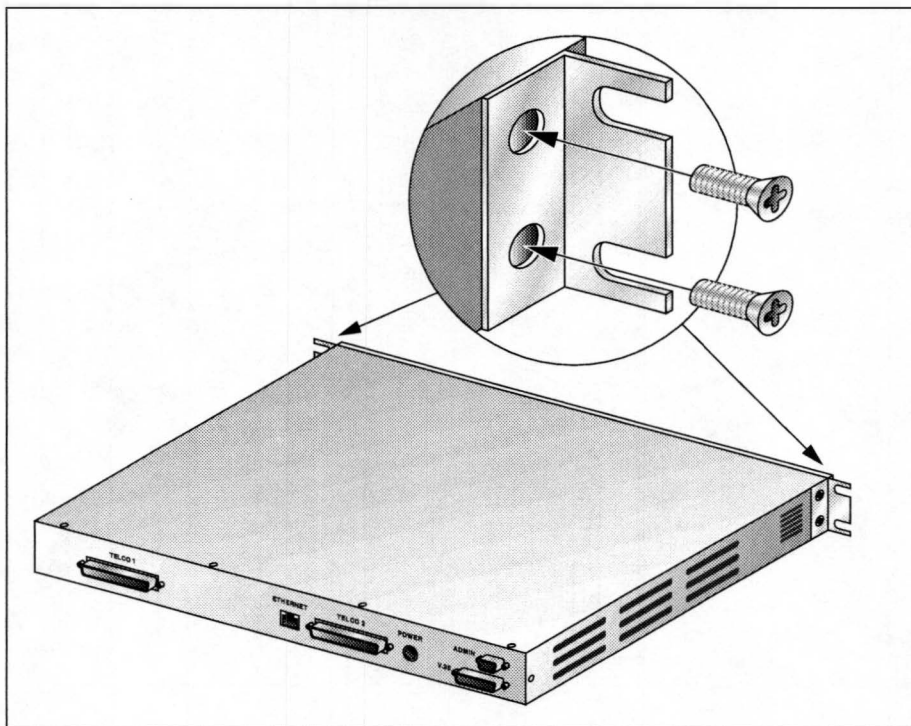
- 6 When you are satisfied that the Remote Office 9150 unit is securely mounted, continue with "Connecting the Remote Office 9150 unit" on page 113.

To install the Remote Office 9150 unit in a rack

The rack slot chosen for the Remote Office 9150 unit must

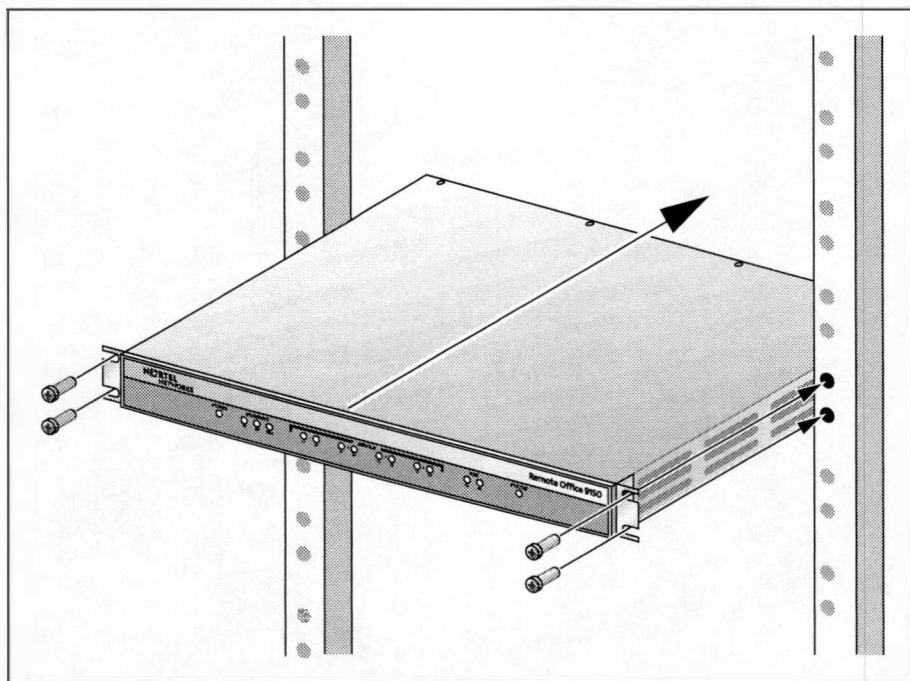
- be large enough to provide air circulation to keep the Remote Office 9150 unit cool
- allow you to securely fasten the Remote Office 9150 unit to the rack using the rack-mount brackets

- 1 Attach the rack-mount brackets as shown in the following illustration.



G101397

- 2 Slide the Remote Office 9150 unit into the rack slot.



G101398

- 3 Secure the Remote Office 9150 unit to the rack with nuts and bolts.
- 4 When you are satisfied that the Remote Office 9150 unit is securely installed, continue with "Connecting the Remote Office 9150 unit" on page 113.

What's next?

When you have completed the installation of the Remote Office 9150 unit in its chosen location, attach the cables. For instructions, see "Connecting the Remote Office 9150 unit" on page 113.

Connecting the Remote Office 9150 unit

When you establish the cabling connections, you are connecting the Remote Office 9150 unit to the:

- power source
- telephones and ISDN BRI trunks

Note: If you are connecting the Remote Office 9150 unit to a Meridian 1 in-building cross-connect system, you need a QCBIX1A BIX block.

- Ethernet network
- administration PC

Remote Office 9150 ISDN BRI Interface information— for Norway and Sweden only

EN 60950:1992 Annex ZB, Special National conditions, Clause 6.2.1.2 states that in Norway and Sweden, supplementary insulation for a primary circuit is required between any TNV circuit and any circuit that has a connection to a protective earthing terminal.

The Remote Office 9150 has the ability to support up to a maximum of 4 ISDN BRI connections. To comply with the aforementioned specification for supplemental insulation, an isolation adapter must be placed between each of the 9150 BRI inputs and the BRI lines from the service provider.

Isolation adapters are available from local vendors. Alternatively, you may order this part from Nortel Networks as a merchandise item. The Nortel Networks part number is P0935714.

Cables you must provide

Ensure that you have obtained the telephone and Ethernet cables for your network. These cables are not supplied in the Remote Office 9150 unit package.

The cables must meet the following requirements:

- telephone cable: One end of the cable must provide a male 50-pin connector. (This end connects to the Remote Office 9150 unit.)
Ensure the other end of the cable matches the connectors needed to connect to the telephones or trunks. (For example, if you are using a BIX block to establish the telephone connections, the wires inside must be exposed.)

Notes:

- Two telephone cables are required, depending on how many telephones and trunks are installed. (Each telephone cable provides support for up to 16 digital telephones, and two ISDN BRI lines providing two B-channels each. The Telco 1 cable also provides support for one analog station such as a fax machine.)
Nortel Networks recommends that you use straight-through Amphenol cables instead of side-entry Amphenol cables. (See “Cable attachment” on page 116.)
- Digital telephones should be located no further than 1230.7 meters (4000 feet) from the Remote Office 9150 unit.
- The analog device should be located no further than 307.7 meters (1000 feet) from the Remote Office 9150 unit.
- Ethernet cable
If you are connecting the Remote Office 9150 unit to a hub, you need a standard CAT5 unshielded twisted-pair (UTP) straight-through Ethernet cable. The cable should be no longer than 100 meters (325 feet) in length.

Connector and pin-out reference

The following table identifies where to find the pin-out table for each connector:

Connector	Connection type	For the pin-out table, see
TELCO 1	25 TIP and RING pairs	page 374.
TELCO 2	25 TIP and RING pairs	page 376.
ETHERNET	RJ-45	page 378.
ADMIN	DB-9	page 379.
Power	DIN	page 380.

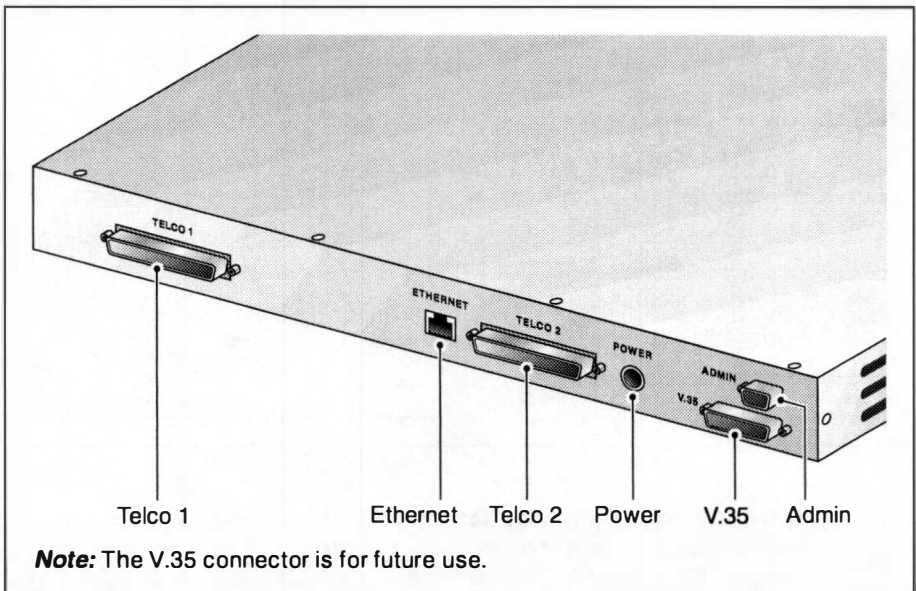
More information

The following documents describe how to establish telephone and trunk connections using the Meridian 1 BIX in-building cross-connect system:

- *Meridian 1 Installation planning* (NTP 553-3001-120)
- *Telephone and attendant console installation* (NTP 553-3001-215)
- *BIX* In-Building Cross-Connect System Material Installation and Servicing (Wall-Mounted System)* (NTP 631-4511-200)

Remote Office 9150 unit connection panel

The following diagram shows the connectors on the back panel of the Remote Office 9150 unit.



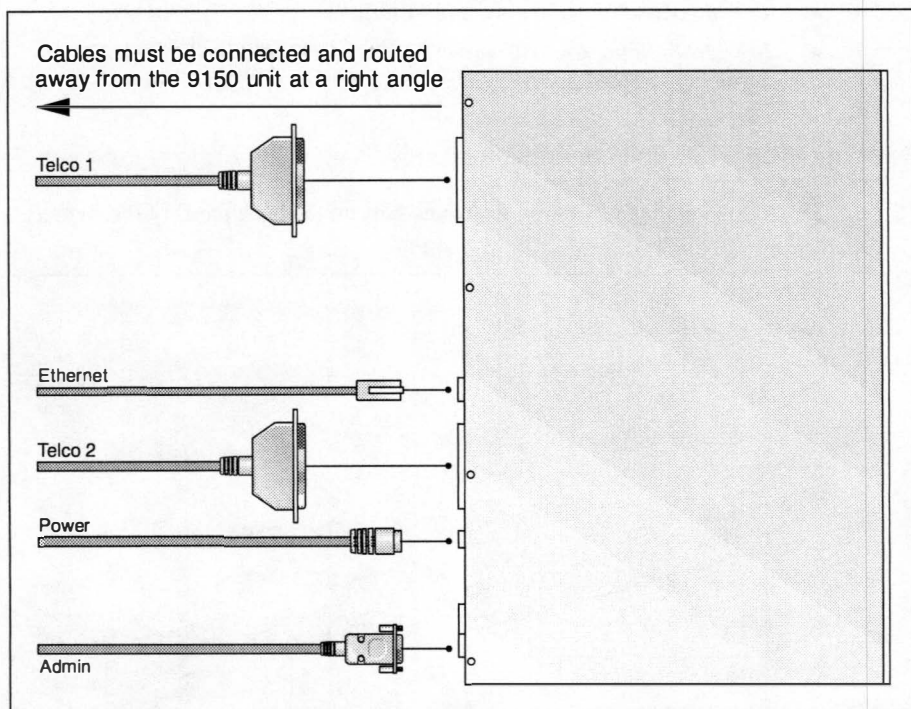
G101403

Note: If you want to connect the Remote Office 9150 unit to an uninterruptible power supply (UPS), ensure the UPS has a minimum of 100 Watts available.

Cable attachment

Nortel Networks recommends that you use straight-through Amphenol cables instead of side-entry Amphenol cables.

The following diagram shows cable attachment.



G101399

Note: The Remote Office 9150 Telco 1 and 2 connections provide the opposite gender of that provided by an Meridian 1 IPE or Option 11 cabinet line card slot. Therefore, different cables must be used when connecting to the Remote Office 9150 than cables used to connect to Meridian 1 line cards.

To connect the Remote Office 9150 unit to the network



WARNING

Risk of electric shock or damage to equipment

To reduce the risk of electric shock to yourself or damage to the Remote Office 9150 unit, ensure that the power source to the unit is turned off until the Telco 1 and Telco 2 connections have been completed.

- 1 Connect the male 50-pin connector of the telephone cable to the TELCO 1 connector on the Remote Office 9150 unit.

Secure the cable connection by snapping the wire tabs into place or by inserting screws.
- 2 Refer to the pin-out table in "TELCO 1 connector pin-out table" on page 374 (in Appendix C) for establishing the connections to the telephones and trunks.
- 3 If you want to route calls over the IP network, or administer the Remote Office 9150 unit from another location on the IP network, connect the Remote Office 9150 unit to the Ethernet network by doing the following:
 - a. Connect one end of the RJ-45 Ethernet cable to the ETHERNET connector on the Remote Office 9150 unit.
 - b. Connect the other end to an Ethernet hub.
- 4 Connect the male 50-pin connector of the other telephone cable to the TELCO 2 connector on the Remote Office 9150 unit.

Secure the cable connection by snapping the wire tabs into place or by inserting screws.
- 5 Refer to the pin-out table in "TELCO 2 connector pin-out table" on page 376 (in Appendix C) to establish the connections to the telephones and trunks.

- 6 Connect the ADMIN connector on the Remote Office 9150 unit to the administration PC as follows:
 - a. Connect the male 9-pin connector of the supplied RS-232 serial cable to the ADMIN connector on the Remote Office 9150 unit.

Note: You may need to provide an RS-232 adapter if the available RS-232 port on your PC does not match the connector on the serial cable.
 - b. Connect the other end to an available COM port on the PC.
- 7 Connect the Remote Office 9150 unit to the power source as follows:
 - a. Connect the four-pin plug on the power transformer to the POWER connector on the Remote Office 9150 unit.

Note: Ensure the arrow on the four-pin plug faces up.
 - b. Connect the AC cord to the AC power receptacle on the power transformer.
 - c. Plug the AC cord into a 110 V or 220 V uninterruptible power source (UPS) or wall outlet.
- 8 Proceed with "Powering up the Remote Office 9150 unit" on page 119.

Powering up the Remote Office 9150 unit

As soon as you connect the Remote Office 9150 unit to the power source, the unit begins to power up.

Note: If you are connecting a Remote Office 9150 unit to a UPS (uninterruptible power supply), ensure that the UPS has a minimum of 100 Watts available.

What happens during power-up

During power up, the following events occur:

- The Remote Office 9150 unit performs a self-test that verifies all critical functionality.
- An LED test sequence is performed.

Power-up self-test

During power-up, the Remote Office 9150 unit performs a self-test that verifies all critical functionality, including

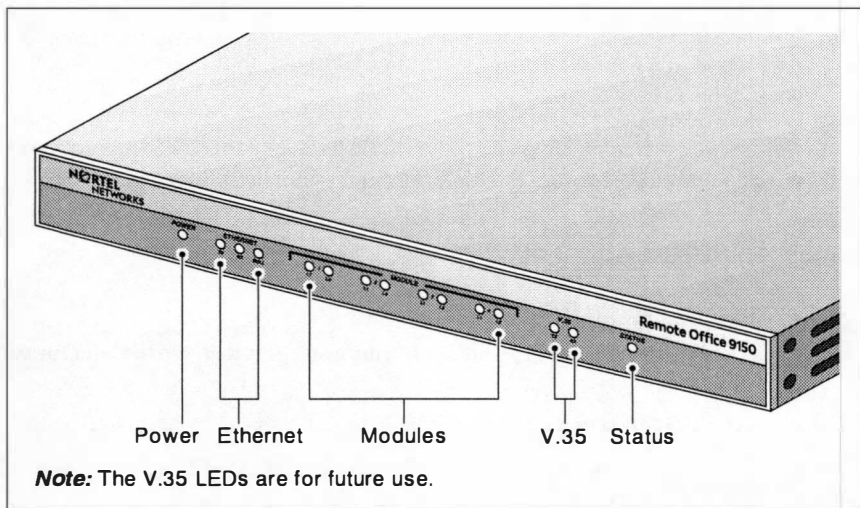
- RAM memory test
- EPROM checksum validation
- flash checksum validation
- DSP health
- interface loopbacks

The power-up cycle also automatically detects if one or more DSP application or trunk interface modules have been installed. If trunk interface modules have been installed, you can configure them in Configuration Manager.

The power-up cycle takes about 60 seconds to complete.

LED test sequence

The following diagram shows the LEDs on the front panel.



G101402

During the power-up cycle, the LEDs behave as follows:

1. All LEDs light for about 15 seconds.
2. The Module LEDs light individually in sequence (1 through 8).
3. All LEDs light.
4. All LEDs except the Status LED go out. The Status LED remains lit.

Note: Steps 2 through 4 take about 4 to 5 seconds.

After this point, the Remote Office 9150 unit is functional.

Notes:

- The ETHERNET TX and RX and module (ISDN BRI) LEDs flash only when transmit and receive activity is present on those interfaces.
- The ETHERNET COLL LED flashes when a data collision occurs on the line.

What's next?

If the power-up cycle completes successfully (indicated by a lit Status LED), your hardware installation is successful. Continue with "Installing the software" on page 122.

If the power-up cycle was not successful (indicated by the Status LED going out), contact your Nortel Networks distributor. There is a possible hardware problem.

Installing the software

You use the Configuration Manager software to configure and administer the Remote Office 9150 unit. This software is located on the CD-ROM provided in the package. You must install the software on the administration PC.

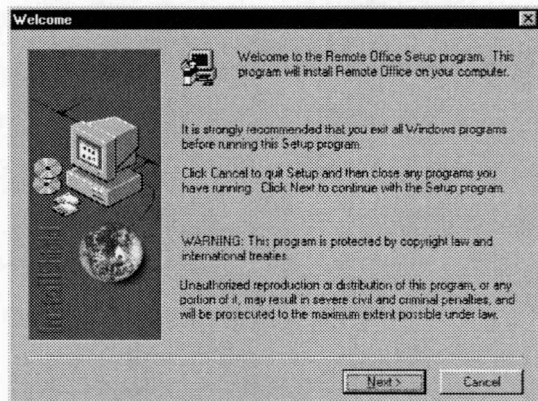
To install the software

- 1 Insert the CD-ROM in the applicable drive on your PC.

Result: If autorun is enabled on your PC, a Welcome screen appears listing available options.

- 2 If autorun has started, select the Install option; otherwise, navigate to the software directory, and then locate and double-click setup.exe.

Result: The InstallShield prepares for installation, and then the Welcome screen appears.



- 3 Click Next, and then follow the screen prompts.

Result: Once the software has been installed, messages appear confirming that the Windows registry has been updated and that the installation was successful.

- 4 Click OK to the next message.

Result: The Setup Complete screen appears.



Note: You might be prompted to restart your computer. If you are, then click Yes, I want to restart my computer.

- 5 Click Finish.

Result: The InstallShield closes.

What's next?

After you install the software on the administration PC, start Configuration Manager and run the Configuration Wizard. The Configuration Wizard allows you to perform initial configuration quickly and easily.

For instructions, see "Using the Configuration Wizard to perform initial configuration" on page 124.

Note: DLL files installed by the Configuration Manager InstallShield should be left in the Windows system directory. Do not move these files to any other directory.

Using the Configuration Wizard to perform initial configuration

The Configuration Wizard option in Configuration Manager allows you to configure the minimum information needed for establishing communications between the Remote Office 9150 unit and the RLC at the host site. The Configuration Wizard does not provide all the configuration settings that are available in Configuration Manager. By using the Configuration Wizard, the Remote Office 9150 unit can be up and running within 10 minutes.

You can use the Configuration Wizard in offline mode or while connected and logged on to the Remote Office 9150 unit (online mode).

What you can configure with the Configuration Wizard

The Configuration Wizard allows you to configure the following:

- the Remote Office 9150 unit's IP address, subnet mask, and default gateway

This information must be valid for your IP network.

Note: If you will not be using the IP network to route calls, you must still enter this information for administration purposes. If you do not have an IP network in place, you can use the sample information provided in the procedure on page 129.

- for Voice over IP capability: the IP address for the RLC at the host site
- for PSTN capability:
 - the telephone number of the RLC at the host site
 - information provided by your ISDN service provider for each ISDN BRI trunk interface module (telephone numbers, SPIDs, and switch type)

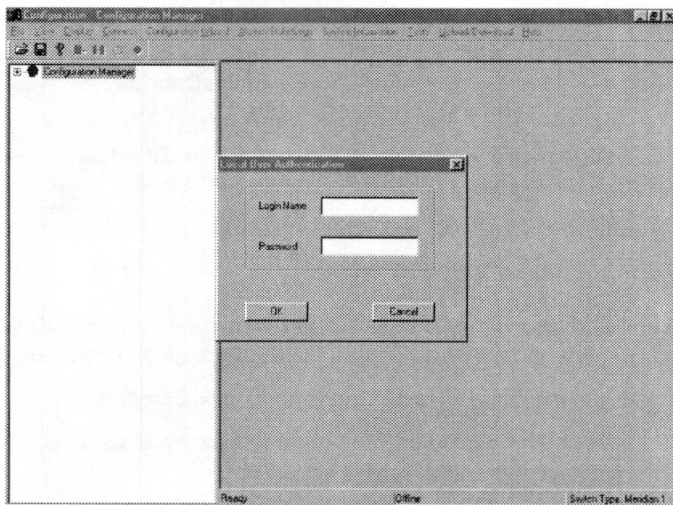
Ensure you have this information ready before you begin.

Note: If, after completing configuration with the Configuration Wizard, you want to modify any settings, you must use Configuration Manager.

To start Configuration Manager

- 1 Click Start → Programs → Remote Office → Configuration Manager.

Result: The Configuration Manager opens and you are prompted for the logon name and password.



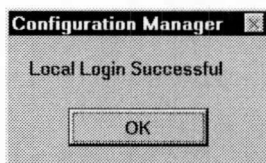
- 2 Enter admin into the Login Name box.

- 3 Enter root into the Password box.

Note: This is the default password. It might be different.

- 4 Click on the OK button.

Result: You are informed if the logon was successful.



- 5 Click OK.

Result: The logon status dialog box disappears.

6 Do one of the following:**IF you want to
perform an****THEN**

offline configuration

do the following:

- a Choose View → Device Type → 9150.
- b Continue with "To perform configuration with the Configuration Wizard" on page 129.

online configuration

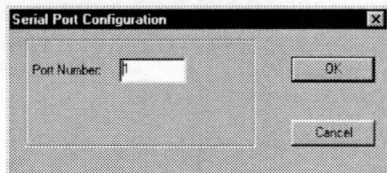
continue with "To establish a serial connection" below.

To establish a serial connection

Note: If you want to perform an offline configuration, ignore this procedure. Go to "To perform configuration with the Configuration Wizard" on page 129.

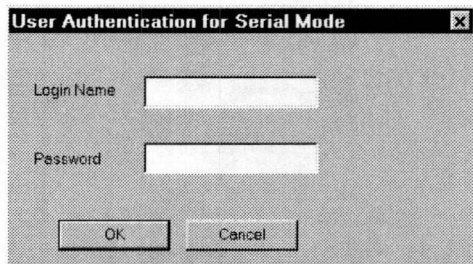
1 From the menu, choose Connect → Login board → Serial.

Result: The Serial Port Configuration dialog box appears.



- 2 Enter the COM port to which the Remote Office 9150 unit is connected, and then click OK.

Result: The User Authentication for Serial Mode dialog box appears.



- 3 Type guest for the logon name.
- 4 Type guest123 for the password.

Note: This is the default password. It might be different if it was changed.

- 5 Click OK.

Result: The connection attempt is initiated. Trying to Connect via Serial Port <port number> might appear.

IF the logon attempt	THEN
----------------------	------

failed	
--------	--

	the following message appears:
--	--------------------------------

SERIAL CONNECTION FAILED

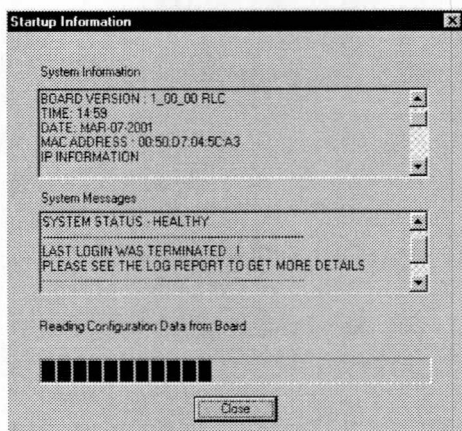
Check the serial connection and ensure it is good.
Then, go back to step 1.

IF the logon attempt THEN

succeeded

the User Logged In dialog box appears.
Click OK.

Result: The following dialog box appears:



The following messages appear above the progress bar at the bottom of the dialog box:

- Reading Hardware Information
- Reading DSP Load Data
- Reading Configuration Data

These messages mean that Configuration Manager is obtaining the unit's configuration information from flash memory.

When initialization completes, click on the Close button.

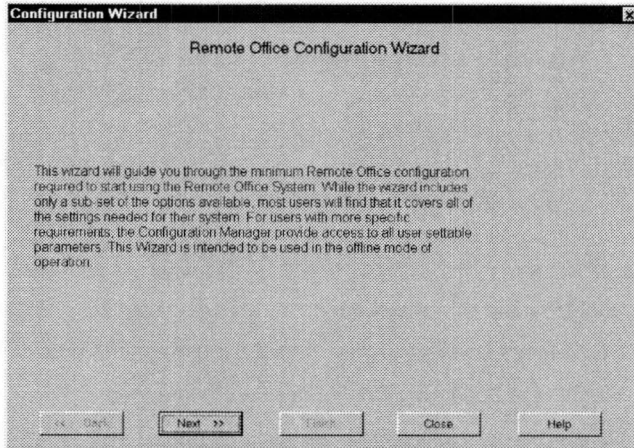
-
- 6 Continue with "To perform configuration with the Configuration Wizard."

To perform configuration with the Configuration Wizard

Note: The screen examples in this procedure use information from the sample network diagram in “Example of a network” on page 360.

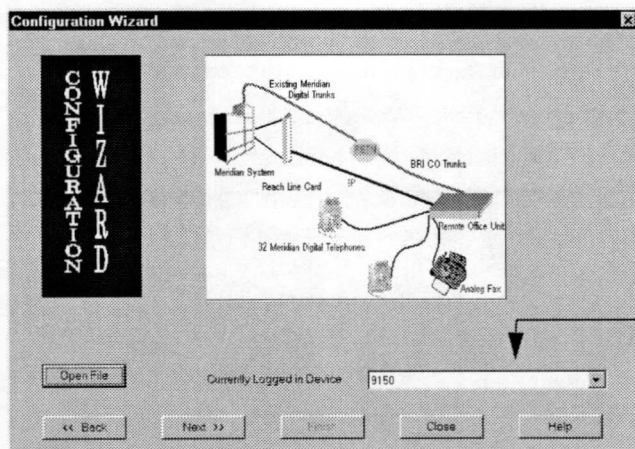
- 1 Choose Configuration Wizard from the menu.

Result: The following screen appears:



- 2 After reviewing the message, click Next.

Result: The following screen appears:



Ensure the
Device box
shows 9150.

- 3 Verify that the Currently Logged in Device box shows 9150, then click Next.
If it does not show 9150, then select 9150 from the list box.
Result: The Local Unit Configuration screen appears.
Note: A completed example is shown on page 131.
- 4 Complete the fields on this screen as described in the following table:

Field	Description
Set the unique Unit ID of the unit	Enter the number from 1–255 that uniquely identifies the Remote Office 9150 unit you are configuring for a particular RLC. Note: Each unit connected to a RLC must be given a unique unit ID. This implies that Remote Office 9150 units that connect to different RLCs in the network can have the same unit ID.
Enter a node name that identifies the unit	Enter a name that uniquely identifies the Remote Office 9150 unit you are configuring.

Field	Description
Enter the local IP Address of the unit	Enter the IP address assigned to the Remote Office 9150 unit. Note: If you do not have a valid IP address, type the sample IP address: 10.1.1.2.
Enter the Local IP Mask of the unit	Enter the subnet mask. Note: If you do not have a valid subnet mask, type the sample subnet mask: 255.255.0.0.
Enter the Local IP Gateway of the unit	Enter the IP address of the gateway between the Remote Office 9150 unit and the network. Note: If there is no router between the Remote Office 9150 unit and the network, then the administration PC acts as the gateway. Type 10.1.1.10. ■ as the IP address on the administration PC ■ as the gateway on the Remote Office 9150 unit

The following is a completed example:

The IP information allows you to administer the Remote Office 9150 unit from any location on the network.

- 5 Click Next.

Result: The Set the Configuration for the Remote Unit screen appears.

Note: A completed example is shown on page 133.

- 6 Complete the fields on this screen as described in the following table:

Field	Description
Set the Unit ID of the RLC to connect to	Enter the RLC's unit ID.
Wish to Enable IP Voice Connection to Remote	■ Accept Yes if the IP network will be used to route calls. Then, enter the IP address of the RLC to which this Remote Office 9150 unit is connected. ■ Click No if the IP network will not be used. The IP Address boxes are dimmed.
Wish to Enable PSTN Connection to Remote	■ Accept Yes if the PSTN will be used to route calls. Then, enter the telephone number that must be dialed to connect to the RLC. The telephone number can include the following digits or characters: 0 through 9, #, *, comma (,), period (.), and dash (-). ■ Caller ID separator: "." (period) ■ Caller ID separator and 1/2 second delay: "," (comma) ■ null separator: "-" (dash) ■ Click No if the PSTN will not be used. The PSTN Number box is dimmed.

Field	Description
Wish to configure Multiple 9150 Ports	- Click Yes if you want to assign Remote Office 9150 ports to digital telephones now. Then, do the following: - Enter the first RLC port number to assign. Note: Nortel Networks recommends that ports be configured so that the RLC port number matches the Remote Office 9150 unit's port number. - Enter the number of telephones connected to the Remote Office 9150 unit. - Click No if you want to complete port assignment at a later time with Configuration Manager.

The following is a completed example:

Click Yes to allow voice calls over IP, then enter the RLC's IP address.

Click Yes to allow voice calls over the PSTN, then enter the RLC's phone number.

Click Yes to automatically assign Remote Office 9150 unit ports to RLC ports, then enter the information as described previously.

7 Click Next.

Result: The Enter the BRI module data screen appears.

Note: A completed example is shown on page 135.

8 Complete the fields on this screen as described in the following table:

Field	Description
Which module would you wish to configure	Click the number identifying the trunk interface module that you are configuring. The number you select must match the position where the module has been installed in the Remote Office 9150 unit.
Module Status	This box identifies if a module has been physically installed on the Remote Office 9150 unit.
Select the Switch Type	Select the type of switch used by your ISDN service provider.
Select the ISDN Line Type	Select the ISDN variant used in your country.
Enter the PSTN Number (B channel 1 and B channel 2)	Enter the telephone number provided by your ISDN service provider for this B-channel.
Enter the SPID Number (B channel 1 and B channel 2)	Enter the Service Profile Identifier (SPID) provided by your ISDN service provider for this B-channel.
B Channel Usage (B channel 1 and B channel 2)	Select one of the following connection types: ■ Local: This trunk is used for local PSTN calls only. ■ Remote: This trunk is used only for calls to and from the host PBX. ■ Local & Remote: This trunk can route both types of calls.

The following is a completed example.

Select the module you want to configure.

Specify the ISDN line and switch type. (Get this information from your service provider.)

Enter the DN and SPID for each B-channel. Then, specify whether the B-channel will be used to process locally controlled calls, host-controlled calls, or both.

9 Repeat step 8 for each ISDN BRI module you want to configure.

10 Click Next.

Result: The following screen appears:

11 Do the following:

IF you are performing an	THEN
--------------------------	------

offline configuration

1 Click Save to File.

Result: You are prompted to specify the directory path and file name for the configuration file.

2 Specify the directory path and file name for this configuration.

Note: The file name is automatically defaulted with the name you entered as the node name.

3 Ensure the Files of type box shows Text File(*.TXT).

4 Click Save to complete the Save to File.

Result: The file is saved, and then you are asked if you want to configure another board. If you do, click Yes, and continue with step 3 on page 130.

The information in this file can be opened in Configuration Manager, and then sent to and saved in the Remote Office 9150 unit's flash memory at another time. For instructions, refer to "Working with configuration files" on page 163.

online configuration

1 Click Save to Flash.

Result: The information entered is written to the flash memory of the Remote Office 9150 unit you are configuring.

If successful, the following message appears:

Data Sent Successfully

Note: Nortel Networks recommends that you also save the configuration to a file.

2 Restart the Remote Office 9150 unit.

What's next?

Now that you have configured the minimum information required for network connectivity, you can do the following:

- Test the network connections. For instructions, see “Testing the network connections” on page 138.
- Perform additional configuration, if needed. For instructions, see Chapter 5, “Configuring the Remote Office 9150 unit.”

Testing the network connections

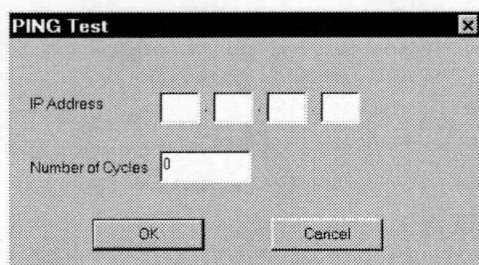
After you have installed the hardware and performed initial configuration, verify that network connectivity is present by performing the tests described in this section.

To verify IP network connectivity using PING

To test the Ethernet connection between the administration PC and the Remote Office 9150 unit, you can use PING. To do this test, the Remote Office 9150 unit and the administration PC must be physically connected to the IP network.

- 1 From the menu in Configuration Manager, choose Tests → Ping.

Result: The PING Test dialog box appears.



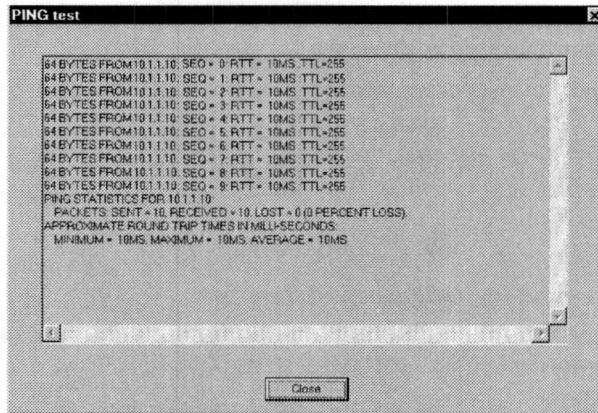
- 2 Enter the IP Address of the unit you want to ping.
- 3 In the Number of Cycles box, enter the number of times you want to ping the unit.

The number must be in the range of 1–100.

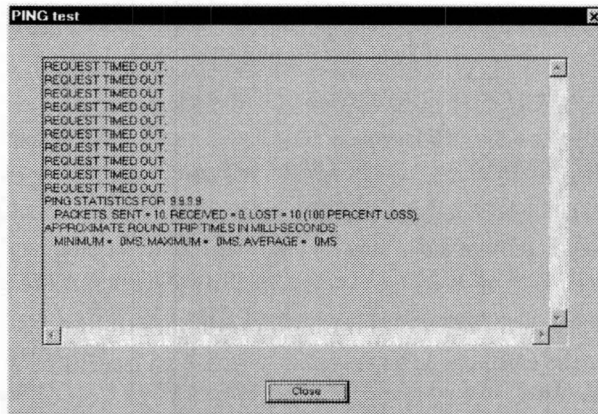
- 4 Click OK.

Result: The PING test results screen appears, showing the ping results.

The following is an example of a successful ping:



The following is an example of an unsuccessful ping:



- 5 Click Close.

Result: The Ping test screen closes.

What to do if the ping did not work

- 1 Use Configuration Manager to ensure you have entered the IP address, subnet mask, and default gateway correctly.

Note: For instructions, see "To enter the IP addresses" on page 196.
- 2 Ping the gateway to see if it responds.
- 3 If the ping still does not work, contact your data network administrator.

To verify the telephone network connectivity

- 1 Look at the digital telephone display.

Does it display the correct time and date? If yes, then the connection paths between the digital telephone, Remote Office 9150 unit, and the RLC are working.
- 2 Lift the telephone handset, or press the host call appearance key to go off hook.

Did you receive a dial tone? If yes, then the connection path between the Remote Office 9150 unit and the RLC is working.
- 3 Initiate an outgoing call through the host PBX.

Did the call proceed as expected? If yes, then the connection path between the Remote Office 9150 unit and the RLC is working.
- 4 Press the local call appearance key to go off hook.

Did you receive a dial tone? If yes, then the connection path between the Remote Office 9150 unit and the digital telephone is working.
- 5 Initiate an outgoing call through the PSTN.

Did the call proceed as expected? If yes, then the ISDN BRI lines to the PSTN are working.

What to do if the telephone connection tests do not work

- 1 Ensure the Remote Office 9150 unit completed its power-up cycle successfully. If it did, the Status LED remains lit.
- 2 Verify the connections between the telephone network and the Remote Office 9150 unit.

- 3 Ensure that the placement of ISDN BRI modules within the Remote Office 9150 unit correspond with the Telco 1 and Telco 2 cable connections.

Note: Refer to the Telco 1 and Telco 2 cable pin-out tables in Appendix C, "Connection pin-out tables."
- 4 Use Configuration Manager to verify that the following configuration is correct on the Remote Office 9150 unit, as appropriate:

- IP addresses (Remote Office 9150 unit, subnet mask, and default gateway, as well as the RLC's IP address, if the IP network is being used to route calls)
- the telephone number used to establish connections to the RLC, if the PSTN is being used to route calls
- the security IDs of both the Remote Office 9150 unit and the RLC, if a security ID is required to authenticate connection attempts
- DNs and SPIDs assigned to the ISDN BRI modules installed in the Remote Office 9150 unit
- station configuration, to ensure that the telephone you are using has the calling capabilities needed to complete the tests (that is, verify that the station is correctly configured as local only, remote only, or both local and remote)

Note: For instructions on using Configuration Manager, see Chapter 5, "Configuring the Remote Office 9150 unit."

- 5 Work with the administrator at the host PBX site to ensure that
 - the RLC is enabled and working in its PBX slot (restart the RLC, if necessary)
 - the configuration of the IP address, telephone number, and security ID on the RLC port are correct (if these items are used)
- 6 Verify that both the telecom and data networks are routing voice calls as expected (that is, calls are not being blocked in any way).

What to do if nothing works

If you cannot get the system to work, contact your Nortel Networks distributor for assistance.

What's next?

Once you have confirmed that the Remote Office 9150 unit can be recognized on the network, you can fine-tune the configuration. Nortel Networks recommends that you also change the passwords used for logging on to the Configuration Manager and the Remote Office 9150 unit.

For	See
a description of Configuration Manager	Chapter 4, "Configuration Manager overview."
instructions on how to modify the configuration	Chapter 5, "Configuring the Remote Office 9150 unit."
instructions on how to change passwords	"Changing the administration password" on page 260.

Chapter 4

Configuration Manager overview

In this chapter

Starting Configuration Manager	144
Configuration Manager description	147
Using the online Help	155
Configuration files description	156
Working with configuration files	163
Selecting the device type for offline configuration	167
Logging on to a unit	169
Logging off from a unit	176
Performing a system restart or shutdown	177
Closing Configuration Manager	180

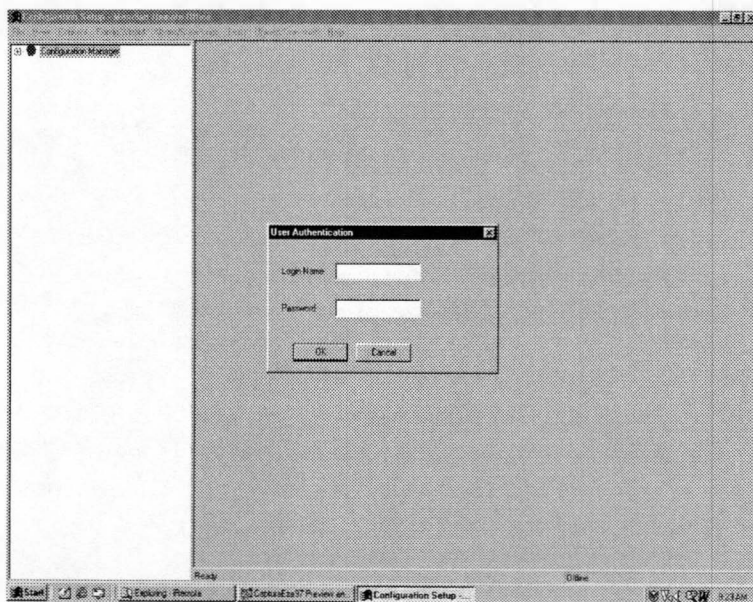
Starting Configuration Manager

To perform administrative tasks, you must first start the Configuration Manager software.

To start Configuration Manager

- 1 Click Start → Programs → Remote Office → Configuration Manager.

Result: The Configuration Manager opens and you are prompted for the logon name and password.



- 2 Type admin in the Login Name box.
- 3 Type root in the Password box.
Note: This is the default password. It might be different.
- 4 Click OK.

Result: You are informed if the logon was successful.

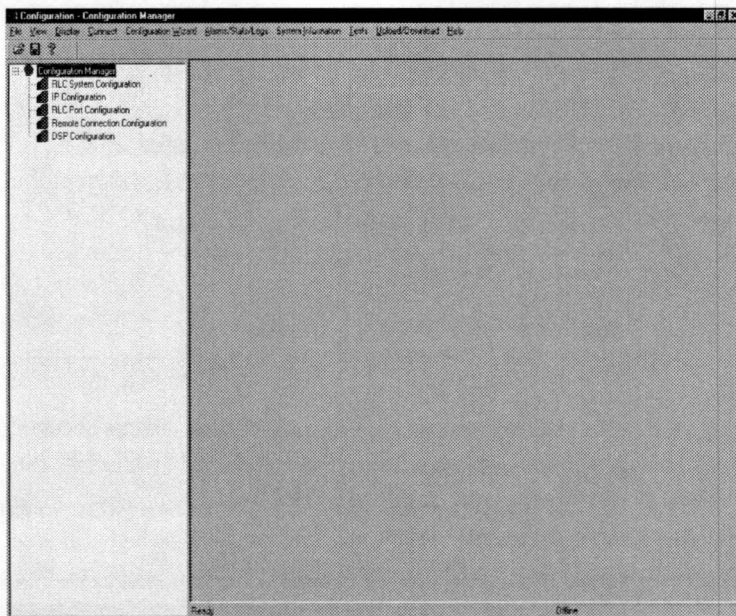
- 5 Click OK.
Result: The Login Name dialog box disappears.

- 6 Proceed as follows:

To perform an	See
online configuration	"Logging on to a unit" on page 169.
offline configuration	"Selecting the device type for offline configuration" on page 167.

- 7 To view the system tree, click the plus sign beside Configuration Manager in the left pane.

Result: Based on the system type you are working with, the system tree expands, showing you the types of configuration you can work with. An example is shown on page 146.



Note: When you first logon to Configuration Manager, the default system tree shows RLC configuration sheets.

Configuration Manager description

This section describes each part of the Configuration Manager screens.

Parts of the Configuration Manager screen

The Configuration Manager is divided into three parts— a menu and two panes.

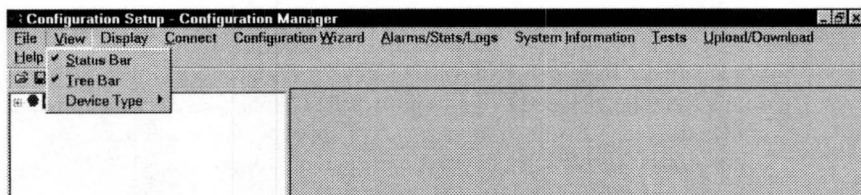
- The menu across the top of the screen lists various administrative tasks you can perform. These tasks are common to all Remote Office units.
- The pane on the left lists the property sheets you can work with. In this guide, the left pane is called the *system tree*.
- The pane on the right displays the screen associated with an item you selected from the system tree. In this guide, the right pane is called the *property sheet*.

Menu

The menu across the top of the screen provides access to system display and reporting options.

When you click an option on the menu, a drop-down list appears. When you select an option from the drop-down list, the screen associated with that option appears.

Note: Options that appear dimmed cannot be used for the unit you are working with, or if you are working offline (that is, when you are not logged on to any unit).



How this guide presents instructions for selecting menu options

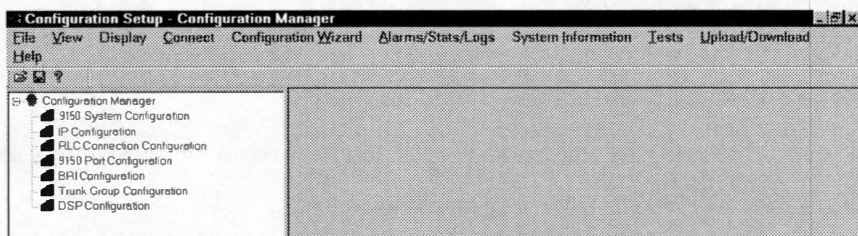
To simplify the instructions for selecting options from the menu, this guide abbreviates the selection path. For example, if a procedure requires you to choose **Over IP** from the **Remote Connectivity** menu, which is under the **Tests** menu, this guide uses the following style:

From the menu, choose **Tests** → **Remote Connectivity** → **Over IP**.

System tree

The left pane of the Configuration Manager lists property sheets you can work with. To view a list of all the property sheets associated with a system, click the plus sign to expand the list. (To hide the list, click the minus sign.)

The following example shows an expanded system tree for the Remote Office 9150 unit:



You can hide the system tree. To do this, choose **View** → **Tree Bar**. The screen redisplay, showing only the property sheet pane.

To display the system tree again, choose **View** → **Tree Bar**.

Property sheets

When you are logged on to a particular system (that is, a Remote Office 9150 unit, a Remote Office 911x series unit, or RLC), and you click an item in the system tree, the associated property sheet appears in the right pane. For instructions on selecting a device type when not logged on, see “Selecting the device type for offline configuration” on page 167.

The following is an example of the property sheet associated with the 9150 System Configuration system tree option:

The screenshot shows a dialog box titled "SYSTEM CONFIGURATION". It contains several input fields and controls:

- Unit ID:** A text box containing the value "1".
- Node Name:** A text box containing the value "9150".
- DSP Gain:** A dropdown menu showing "0" and a small "dB" label.
- Time Offset:** A text box containing "0" with up and down arrow buttons.
- Emergency Activation Code:** A text box containing "911".
- SPRE Codes:** A section containing four text boxes: "Online" (value "39"), "Paging" (value "05"), "Registration" (value "97"), "Offline" (value "98"), "Local Calling" (value "8"), and "DeRegistration" (value "96").
- Trunk Support:** A dropdown menu showing "64K".
- Local SwitchOver:** Two radio buttons, "Enable" and "Disable", with "Disable" selected.
- Companding Algorithm:** A dropdown menu showing "Automatic".
- Multiple Subscriber Number:** Two radio buttons, "Enable" and "Disable", with "Enable" selected.
- International Tones:** A button.
- Buttons:** At the bottom are five buttons: "OK", "Default", "Send", "Retrieve", and "Help".

How this guide presents instructions for displaying property sheets

To simplify the procedures for accessing property sheets throughout this guide, the instructions for displaying a particular property sheet are summarized into a "Getting there" statement.

The procedure for displaying the screen you need depends on whether you are

- performing an online configuration (that is, you are connected to a unit by serial port or Telnet)
- performing an offline configuration (that is, you are not connected to a unit)
- working with the system tree visible

Example

Getting there 9150 → Configuration Manager → IP Configuration

The following is the long instruction for this example:

1 Do the following:

IF you are performing an	THEN
offline configuration	select the 9150 device type as described in "Selecting the device type for offline configuration" on page 167.
online configuration	connect to, and then log on to the Remote Office 9150 unit as described in "Logging on to a unit" on page 169.

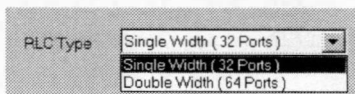
2 Navigate to the IP Configuration screen as follows:

IF the system tree is	THEN
visible	do the following: - a Click the plus sign beside Configuration Manager to expand the system tree. - b Click IP Configuration.
hidden	from the menu, choose Display → IP Configuration.

Result: The IP Configuration property sheet appears in the right pane.

Drop down list boxes

Boxes that provide a limited list of values are called *drop down list boxes*. To view the values available for a list box, click the down arrow for that list box. To select an item from the list, move the cursor until the desired item is highlighted, and then click the item. The item you select appears in the list box.



In some cases, selecting a particular list item causes the property sheet contents to change as follows:

- Some fields appear dimmed (disabled) because they cannot be configured in the context of the list item you selected.
- Other fields are re-enabled (no longer appear dimmed).
- One or more values on the property sheet are replaced with values that are specific to the item you selected.

Check boxes

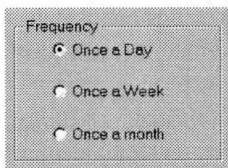
Fields that contain a blank box beside them are called *check boxes*. These check boxes are used to enable or disable the feature associated with that field. To enable the feature, click the check box. A check mark appears. When you click the check box again, the check mark disappears (thereby disabling the feature).



Option buttons

Some fields can have two or more options from which to select. The options contain a circle beside them, which are called *option buttons*. For these fields, only one option can be selected.

To enable an option, click the button for the option you need. If the option you selected is a change, the button for the previously selected option is cleared.



In some cases, selecting a particular option button causes the property sheet contents to change as follows:

- Some fields appear dimmed (disabled) because they cannot be configured in the context of the option you selected.

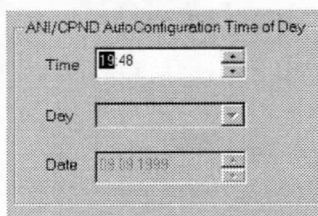
- Other fields are re-enabled (no longer appear dimmed).
- One or more values on the property sheet are replaced with values that are specific to the option you selected.

Scroll boxes

Boxes that contain data with up and down arrows beside them are called *scroll boxes*. When you click the data, and then the up arrow, the selected data increases in value. When you click the down arrow, the selected data decreases in value.

You can also change the data by manually entering it. To do so, highlight the data you want to change, and then type over it.

The following screen is an example of a scroll box:

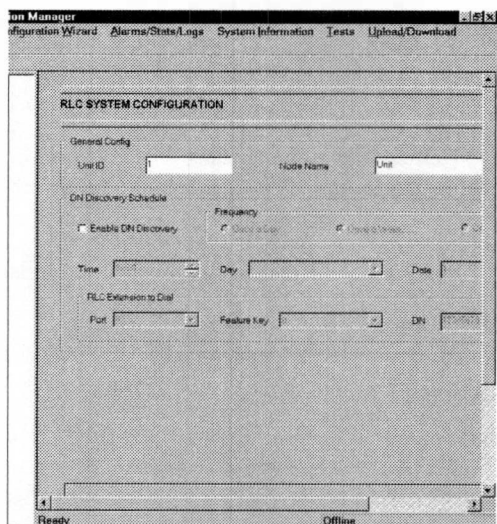


Scroll bars

If your monitor's display settings are configured so that not all the information can be displayed at once, horizontal and vertical scroll bars might appear in Configuration Manager. Some fields and buttons might be hidden. An example is shown on the next page.

The Configuration Manager software application is best viewed when your monitor settings are configured as 1024 by 768 pixels using Small Fonts at 96 dpi. This ensures that all fields and buttons are visible.

For instructions on changing your display settings, refer to the Windows online Help on your PC.



You can prevent these scroll bars from appearing by changing the screen area pixel and font sizes in the Windows Control Panel display settings on your PC.

Command buttons

The following command buttons appear on all property sheets:

- **OK**
OK accepts any changes you make and stores them in a temporary file on your PC until you are ready to update the unit's flash memory. For more details, see "OK" on page 159.
- **Default**
Default replaces the values displayed on the property sheet with default values.
- **Send**
Send updates to the buffer of the unit to which you are logged on with any changes you have made to the configuration. For more details, see "Send" on page 160.

- **Retrieve**
Retrieve downloads the unit's configuration from flash memory and displays it in Configuration Manager on your PC. For more details, see "Retrieve" on page 160.
- **Help**
Help displays online Help for the property sheet you are working with. For other methods of displaying Help, see "Using the online Help" on page 155.

Note: If the command buttons are not visible, use the vertical scroll bar to scroll through the screen.

Using the online Help

While using Configuration Manager, you might have questions about what certain boxes and buttons do, as well as how to complete certain tasks. Online Help provides brief answers to such questions.

To access Help

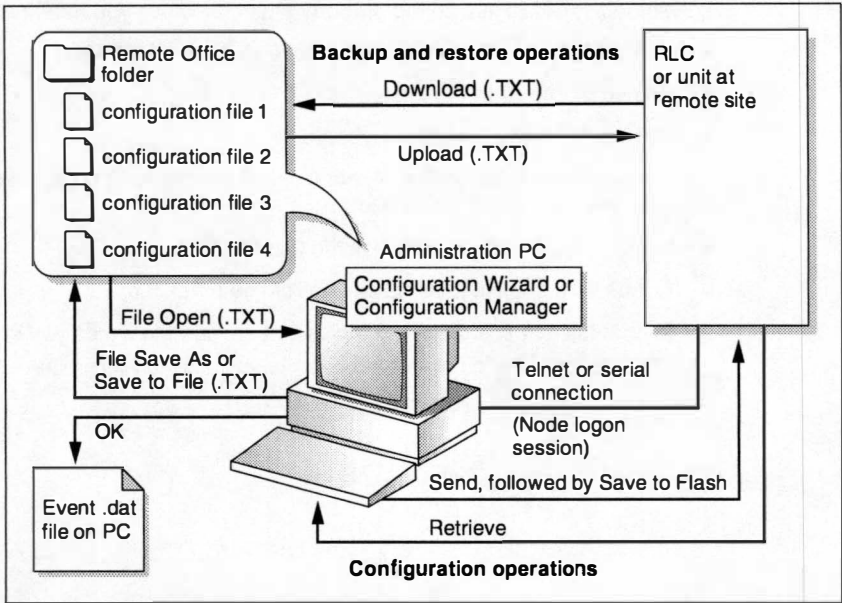
- 1 Use one of the following methods:
 - Method 1: Click Help on the property sheet for which you need help.
 - Method 2: From the Help menu, choose Help → Help Topics.
 - Method 3: Click ? in the toolbar.
 - Method 4: Press F1 on the keyboard.
- 2 If you selected methods 2, 3, or 4, go to one of the following tabs, based on how you want to search for a topic:
 - To see a list of Help topics, click the Contents tab.
 - To look up a subject alphabetically, click the Index tab.
 - To do a full-text search to find topics that contain the words you enter, click the Find tab.

Configuration files description

This section describes configuration files and the ways in which you can work with them.

Configuration Manager: File operations diagram

The following diagram shows how configuration information is stored. A detailed description of each file type and operation follows.



Types of files

There are four types of files that you can work with in Configuration Manager. Each file is identified by one of the following file name extensions as described in the following table:

File name	File type	When it is created and used
EVENT.DAT	Log file	This file records all activities (and messages associated with those activities) that you perform while running Configuration Manager, such as ■ logging on to Configuration Manager ■ logging on to a unit (by serial or Telnet connection) ■ logging off from the unit ■ performing configuration changes ■ performing firmware upgrades This file can be very useful when performing troubleshooting for system problems. If you need technical support, you might be asked to provide this file. Note: Information is appended to this file each time you start a new Configuration Manager session.
*.txt	Text	The text file is created when you do one of the following: ■ Click Save to File while running the Configuration Wizard. ■ Click File → Save As while working in Configuration Manager. ■ Choose Upload/Download → Download Configuration to save a unit's configuration in a text file on the administration PC.

File name	File type	When it is created and used
*.txt (continued)	Text	To view or make changes to the text file (while in online or offline mode), do one of the following to open the file: ■ Click Open while running the Configuration Wizard. ■ Click File → Open while running Configuration Manager. ■ Choose Upload/Download → Upload Configuration to load the configuration file to the unit's buffer. For more details about these tasks, see ■ “Working with configuration files” on page 163 ■ “Performing backups and restores” on page 265. Note: You can view or edit the contents of the text file by opening it in a word processing application, such as WordPad.
*.UPG	Upgrade	Use this file type when performing firmware upgrades. For more details, see “Performing upgrades” on page 309.

Configuration Manager: File operations description

The following table describes each operation shown in the previous diagram:

Operation	Description
OK	When you click OK, the following occurs: ■ The changes you make are checked for errors. If errors are found, an error dialog box appears. Make the necessary changes, and then click OK again. ■ The changes you make are stored in the event.dat file on your PC. For more information about the event.dat file, see “Types of files” on page 157. To update the flash memory of the unit to which you are logged on, you must click Send, and then perform a Save to Flash. For more details, see “Send” on page 160. Note: If you do not click OK on a property sheet before displaying another property sheet, all changes made on the property sheet are lost and must be reentered.
File → Open	When you choose File → Open from the Configuration Manager menu, you can open a previously saved configuration file. This is useful for preparing and storing configuration files in a central location before they are deployed to the network. Note: To open a file, the file type must be text (.txt).
File → Save As	When you choose File → Save As from the Configuration Manager menu, the unit’s configuration is saved to a configuration file on your PC. You specify the file name and directory location. After you save the file, you can open and modify the file at another time. Notes: ■ The file is saved as a text (.txt) file. ■ If you close Configuration Manager without performing a File → Save As, all changes you made are lost.

Operation	Description
Send	When you click Send on the current property sheet, any changes you make to this property sheet are sent to the buffer on the unit to which you are connected. If the send is successful, <code>Data Sent Successfully</code> appears. Note: You must perform a Save to Flash from the Upload/Download Menu to save the changes in the unit's flash memory. For more details, see Save to Flash below.
Send All	When you choose Upload/Download → Send All on any property sheet, changes for <i>all</i> property sheets are sent to the buffer on the unit to which you are connected. If the send is successful, <code>Data Sent Successfully</code> appears. Note: You must perform a Save to Flash from the Upload/Download Menu to save the changes in the unit's flash memory. For more details, see Save to Flash below.
Retrieve	When you click Retrieve on a property sheet, the configuration stored on the unit to which you are connected appears in Configuration Manager. If the retrieve is successful, <code>Data Received Successfully</code> appears.
Save to Flash	When you choose Upload/Download → Save to Flash, the information stored in the unit's buffer is saved to flash memory. This prevents the configuration from being lost if a power loss occurs on the unit. While in progress, <code>Save to Flash in Progress</code> appears in the status bar at the bottom of the screen. When the save to flash is completed, the Data Stored to Flash dialog box appears. Note: You must perform a Send or Send All before you perform a Save to Flash. You should perform a Save to Flash as often as required.

Operation	Description
Upload Configuration	When you choose Upload/Download → Upload Configuration from the Configuration Manager menu, the configuration file you specify is uploaded and written to the buffer on the unit to which you are connected. Use this option if you need to restore or replace an entire configuration. You must perform a Save to Flash from the Upload/Download Menu to save the changes in the unit's flash memory. If you do not perform a Save to Flash and a power loss occurs on the unit, the changes are lost. While in progress, Save to Flash in Progress appears in the status bar at the bottom of the screen. When the Save to Flash is completed, the Data Stored to Flash dialog box appears. Notes: ■ To upload a configuration file, the file type must be text (.txt). ■ To perform a configuration upload over the IP network, a TFTP server application must be running on your PC. Uploads over the serial port are not supported. ■ The upload operation does not affect the event.dat file on the PC. ■ The new configuration does not take effect until you restart the unit. For instructions on how to restart the unit, see "Performing a system restart or shutdown" on page 177.

Operation	Description
Download Configuration	When you choose Upload/Download → Download Configuration from the Configuration Manager menu, the configuration stored on the unit to which you are connected is saved to a file on the PC. Use this option if you want to create a backup of the unit's configuration. Notes: ■ The downloaded file is saved as a text file (.txt). ■ The download operation does not affect the event.dat file on the PC. Therefore, if you make changes and do not save them, they are lost.

Working with configuration files

This section explains how to

- create a configuration file (see page 164)
- open a configuration file in Configuration Manager (see page 165)
- perform a configuration upload (see page 166)
- perform a configuration download (see page 166)

When to use the Configuration Manager file operations

You can use	When you are
OK, File → Open, and File → Save As	working in offline mode or connected and logged on to a unit. Note: When working in offline mode, you must save the configuration to a file. However, when you are connected and logged on to a unit, the file save operation is optional when you use Send or Send All to update the unit's flash memory.
one of the following: ■ Send ■ Send All ■ Retrieve ■ Upload Configuration ■ Download Configuration	connected and logged on to a unit.

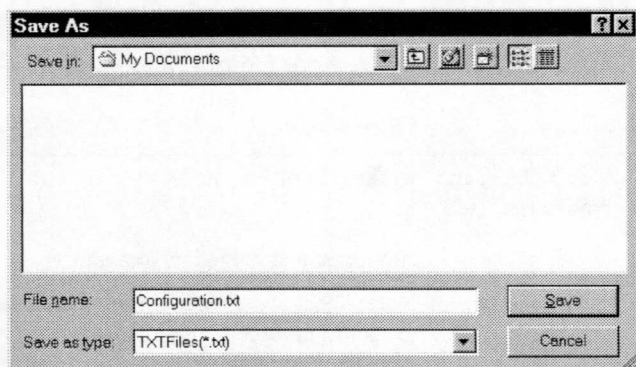
To create a configuration file on the PC

- 1 Start Configuration Manager.
- 2 Make the required changes on each property sheet.

Note: You do not have to be logged on to a unit to make configuration changes. When you are not logged on to a unit, you are performing an offline configuration.

- 3 From the menu, choose File → Save As.

Result: The Save As dialog box appears.



- 4 Enter a descriptive name for the file.

It should identify the type of configuration it contains.

Example 1: If the file contains basic configuration that will be used for all similar-type units, you can type template as the file name.

Example 2: If the file contains configuration that is unique to a specific unit, enter the unit's name or number as the file name.

- 5 Ensure the Save as type box shows Text Files(*.TXT).
- 6 Specify the folder where the file is to be saved.

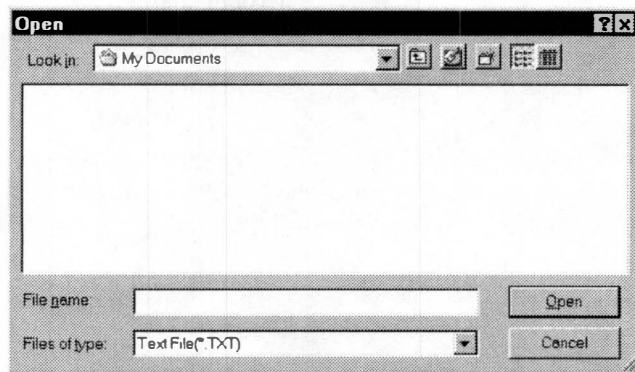
- 7 Click OK.

Result: The file is saved.

To open a configuration file

- 1 Start Configuration Manager.
- 2 If you want to work in online mode, log on to the unit. Otherwise, ensure that you have selected the device type.
- 3 From the menu, choose File → Open.

Result: The Open dialog box appears.



- 4 Ensure the Files of type box shows Text Files(*.TXT).
- 5 Navigate to the folder containing the file you need.
- 6 Select the file, and then click Open.

Result: The contents of the configuration file are loaded into Configuration Manager.

- 7 View the configuration details by clicking each item in the system tree to display the associated property sheet.

- 8 Make changes as necessary, and then do one of the following:
 - a. Save the file.
 - b. Click Send to update the unit, and then perform a Save to Flash.

To upload a configuration to a unit

For instructions, see “Restoring the configuration” on page 268.

To download a configuration from a unit

For instructions, see “Creating a backup configuration file” on page 266.

Selecting the device type for offline configuration

If you are not logged on to a particular system (that is, an RLC, a Remote Office 911x series system, or a Remote Office 9150 system), you must select the type of device with which you want to work.

When you select the device type, it causes the Configuration Manager application to automatically reorganize the system tree with the screens associated with that device type.

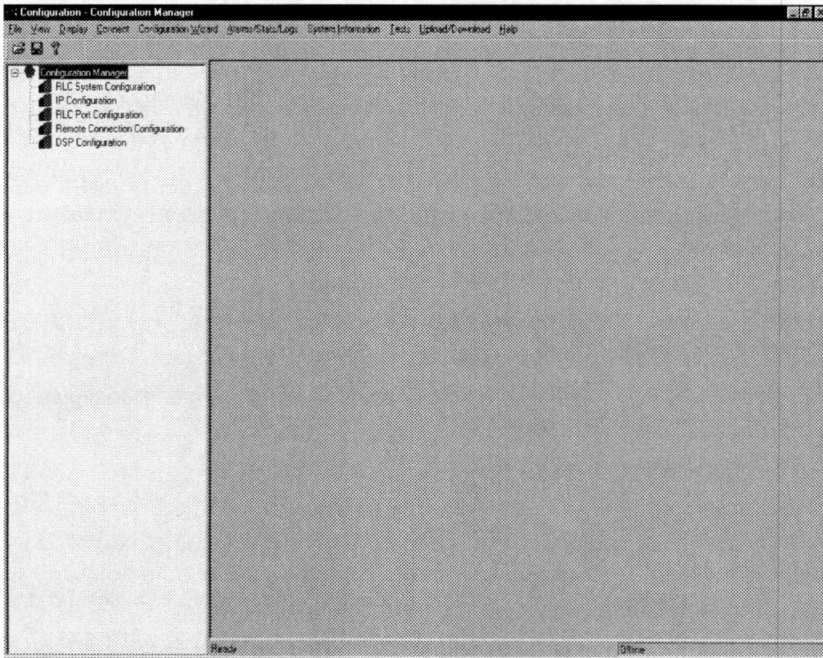
To select the device type

- 1 Start Configuration Manager as described in "Starting Configuration Manager" on page 144.
- 2 Do the following:

To view the system tree for	Do the following
the RLC	Choose View → Device Type → RLC.
the Remote Office 9150 unit	Choose View → Device Type → 9150.

- 3 Click the plus sign beside Configuration Manager in the left pane.

Result: The system tree expands, showing you the types of configuration you can work with, as shown in the example on page 168.



Logging on to a unit

If you want to update the flash memory on a unit as you make configuration changes, or view statistics and logs, you must log on to the unit. Each unit has its own administration ID and password.

You can log on to the unit by using one of the following connection methods:

- Telnet (over the IP network)
- serial port

Connection types

If the RLC or Remote Office 9150 unit is connected to the administration PC by the RS-232 cable, you can establish a connection through the serial port.

If Ethernet connectivity has been established between the administration PC and the RLC or Remote Office 9150 unit, you can establish an IP connection with Telnet.

Connection history

The Configuration Manager maintains a history of past unit connections. You can select and then connect to a unit from the history list that appears in the Connect menu.

Note: The connection history list is deleted each time you upgrade the Configuration Manager software.

Default logon ID and password

The default logon ID is **guest**. It cannot be changed.

The default password is **guest123**. The password can be different if it was changed.

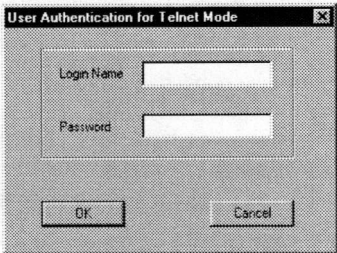
Auto logoff

If the connection has remained active with no activity for 15 minutes or more, you are automatically logged off and the Session Timed Out message appears. This helps to secure the configuration in the event that you walk away from the administration PC while logged on to a unit.

To log on to a unit using the connection history

- 1 From the menu, choose Connect → IP address of the unit to which you want to log on.

Result: The User Authentication for Telnet Mode dialog box appears.



- 2 Enter your logon name and password, and then click OK.

Result: The connection attempt is initiated. Trying to Connect to <IP address> message might appear.

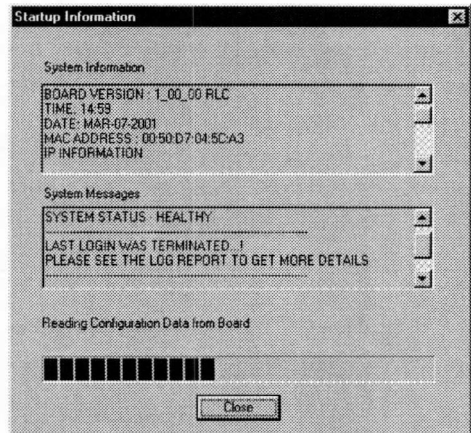
IF the logon attempt	THEN
failed	the following message appears: 10060 TELNET CONNECTION FAILED Go back to step 1.

IF the logon attempt
succeeded

THEN

the User Logged In dialog box appears.
Click OK.

Result: The following dialog box appears:



The following messages appear above the progress bar at the bottom of the dialog box:

- Reading Hardware Information
- Reading DSP Load Data
- Reading Configuration Data

These messages mean that Configuration Manager is obtaining the unit's configuration information from flash memory.

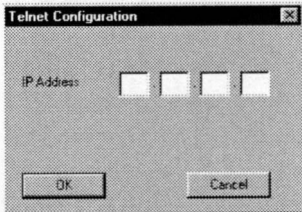
When initialization completes, click on the Close button.

To log on to a unit using Telnet

Note: If someone else is already logged on to the unit, you cannot log on.

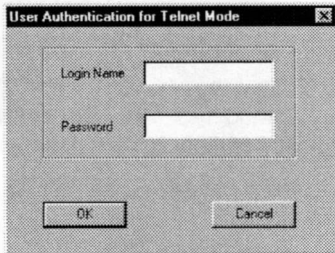
- 1 From the menu, choose Connect → Logon Unit → Telnet.

Result: The Telnet Configuration dialog box appears.



- 2 Enter the IP Address of the unit to which you want to connect and click OK.

Result: The User Authentication for Telnet Mode dialog box appears.



- 3 Enter your logon name and password, and then click OK.

Result: The connection attempt is initiated. The message Trying to Connect to <IP address> message might appear.

IF the logon attempt	THEN
----------------------	------

failed

the following message appears:

10060 TELNET CONNECTION FAILED
Go back to step 1.

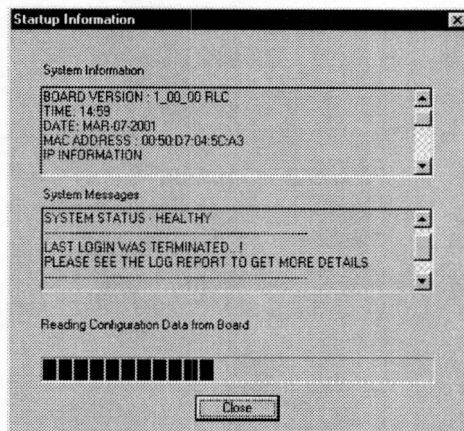
IF the logon attempt THEN

succeeded

the User Logged In dialog box appears.

Click OK.

Result: The following dialog box appears:



The following messages appear above the progress bar at the bottom of the dialog box:

- Reading Hardware Information
- Reading DSP Load Data
- Reading Configuration Data

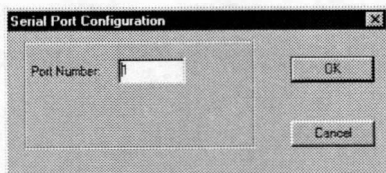
These messages mean that Configuration Manager is obtaining the unit's configuration information from flash memory.

When initialization completes, click on the Close button.

To log on to a unit using the serial port

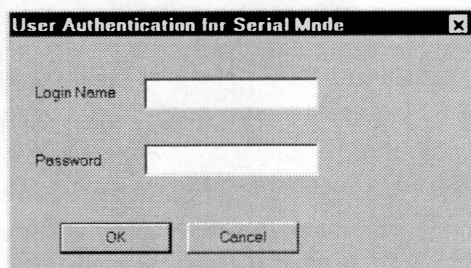
- 1 From the menu, choose Connect → Logon Unit → Serial.

Result: The Serial Port Configuration dialog box appears.



- 2 Enter the COM port number to which the unit is connected, and then click OK.

Result: The User Authentication for Serial Mode dialog box appears.



- 3 Enter your logon name and password, and then click OK.

Result: The connection attempt is initiated. The message Trying to Connect via Serial Port <port number> might appear.

IF the logon attempt THEN

failed

the following message appears:

SERIAL CONNECTION FAILED

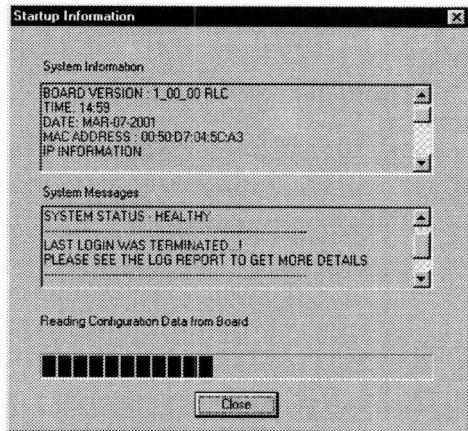
Check the serial port connection and ensure it is good. Then, go back to step 1.

IF the logon attempt
succeeded

THEN

the User Logged In dialog box appears.
Click OK.

Result: The following dialog box appears:



The following messages appear above the progress bar at the bottom of the dialog box:

- Reading Hardware Information
- Reading DSP Load Data
- Reading Configuration Data

These messages mean that Configuration Manager is obtaining the unit's configuration information from flash memory.

When initialization is completed, click on the Close button.

To access property sheets associated with the unit

- 1 Click the plus sign beside Configuration Manager.
Result: This expands the system tree.
- 2 Click the name of the property sheet with which you want to work.
Result: The property sheet appears in the right pane.

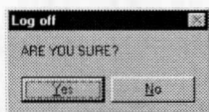
Logging off from a unit

When you are finished using Configuration Manager to make configuration changes, or to view logs and statistics, you should log off from the unit. Logging off secures the unit's configuration.

To log off from the unit

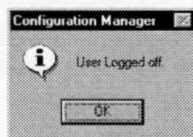
- 1 From the menu, choose Connect → Logoff Unit.

Result: The Log off dialog box appears.



- 2 Click Yes.

Result: The following dialog box appears:



- 3 Click OK.

Performing a system restart or shutdown

Configuration Manager allows you to perform a controlled system restart or shutdown.

When to perform a restart

You must perform a system restart each time you change the configuration or upgrade the firmware.

When to perform a shutdown

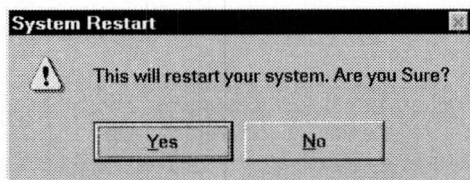
You must perform a system shutdown when

- you want to install DSP application or trunk interface modules
- you need to power down the system for any reason

To perform a system restart

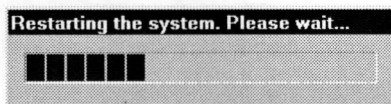
- 1 From the menu, choose Connect → System Reset → Restart.

Result: The System Restart dialog box appears.



- 2 Click Yes.

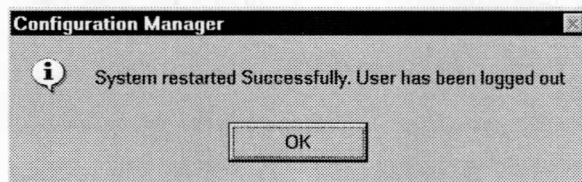
Result: The following status dialog box appears:



The following message also appears in the status bar at the bottom of the screen:

Restarting the System

The status continues to show Online. When the system restart is completed, the following dialog box appears to inform you that the system restart was successful and that you were logged off:



- 3 Click OK.

Result: You are prompted to log back on using the previous connection method (Serial or Telnet).

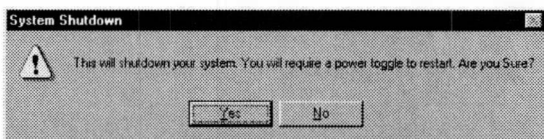
To perform a system shutdown

ATTENTION

Do not perform this procedure if you do not have physical access to the unit. To recover from the system shutdown, you must power the unit off, and then power it back on.

- 1 Choose Connect → System Reset → Shutdown.

Result: The System Shutdown dialog box appears.



- 2 Click Yes.

Result: Your logon session is disconnected, and the following message appears in the status bar at the bottom of the screen:

Shutting Down the System

The status shows Offline.

- 3 Turn the power off.

Note: You must turn the power off before you can power the unit back up.

Closing Configuration Manager

When you have completed all the configuration modifications you want to make, or are done viewing unit logs and statistics, close the Configuration Manager application. This secures the configuration, preventing others from accessing it if you walk away from the administration PC while logged on to a unit.

To close Configuration Manager



CAUTION

Risk of configuration loss

If you close Configuration Manager without saving the changes you made to a file on your PC, or without updating the flash memory of the unit you were working on, all changes are lost. You must reenter any changes you made.

- 1 Ensure that you have saved all configuration changes by doing one or more of the following:
 - From the menu, choose File → Save As, and then specify the name for the configuration file. The file is saved on the administration PC hard disk.
 - Update the flash memory of the unit to which you are connected by doing one of the following:
 - Click Send on any property sheet, and then choose Upload/Download → Save to Flash.
 - Click Send All on any property sheet, and then choose Upload/Download → Save to Flash.
 - If you have saved the changes to a file, choose Upload/Download → Upload Configuration.
For instructions, see "Restoring the configuration" on page 268.

- 2 Log off by choosing Connect → Logoff Unit.
- 3 From the menu, choose File → Exit.

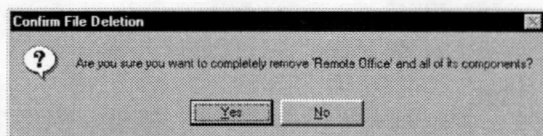
Result: The Configuration Manager closes.

Uninstalling the Configuration Manager software

If you need to remove the Configuration Manager software from your administration PC, do the following:

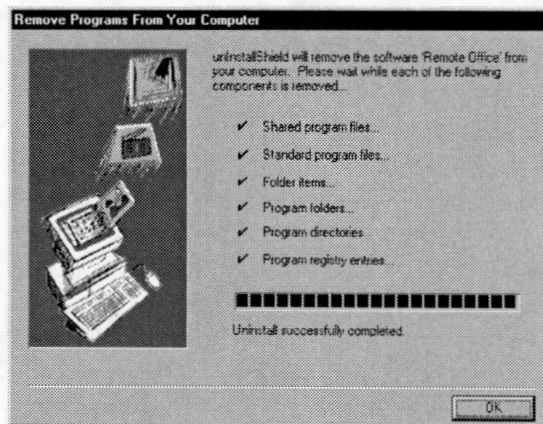
- 1 Click Start > Settings > Control Panel.
- 2 Double-click Add/Remove Programs.
- 3 Select Remote Office from the list, and then click Add/Remove.

Result: The following dialog box appears:



- 4 Click Yes.

Result: The Uninstall Shield begins the uninstall and displays the progress. When the uninstall is completed, the screen appears as follows:



Chapter 5

Configuring the Remote Office 9150 unit

In this chapter

Configuring the system settings	184
Configuring International Tones	190
Configuring the Remote Office 9150 unit's IP interface	195
Configuring the RLC connection information	198
Configuring the PSTN connection number	202
Configuring the security level	204
Configuring trunks and trunk groups	208
Configuring stations	219
Configuring a fax station	231
Configuring DSP resources	235

Configuring the system settings

This section describes the settings that apply to the system rather than to the RLC port or Remote Office 9150 trunks or stations.

Getting there 9150 → Configuration Manager → 9150 System Configuration

System Configuration sheet

SYSTEM CONFIGURATION		
Unit ID	Node Name	
1	9150	
DSP Gain	dB	
0		
Time Offset	Emergency Activation Code	
0	911	
SPRE Codes		
Online	Paging	Registration
# 99	# 05	# 97
Offline	Local Calling	DeRegistration
# 98	# 8	# 96
Trunk Support	Local SwitchOver	
64K	☐ Enable ☒ Disable	
Companding Algorithm	Multiple Subscriber Number	
Automatic	☒ Enable ☐ Disable	
International Tones		
OK	Default	Send
Retrieve		Help

To configure the Remote Office 9150 system settings

- 1 Complete the fields as described in "9150 System Configuration field descriptions" on page 186.
- 2 Click OK to save the information in the temporary work file.
- 3 To update the Remote Office 9150 unit with the new information, click Send.

IF you are**THEN**

logged on to the
Remote Office 9150 unit

the changes are written into the Remote
Office 9150 unit's buffer.

To save the changes in flash memory, choose
Upload/Download → Save to Flash.

not logged on to the
Remote Office 9150 unit

the Connection not Established dialog box
appears:

Do one of the following:

- Log on to the Remote Office 9150 unit,
and then click Send again.
 - Save the changes to a file on your
administration PC.
-

9150 System Configuration field descriptions

Field	Description
Unit ID	Enter a unique number between 1 and 255 to identify this Remote Office 9150 unit. This number must be different from: ■ the number assigned to the RLC where this Remote Office 9150 unit connects ■ the numbers assigned to other remote units connected to the same RLC
Node Name	Enter your site name. The node name uniquely identifies this Remote Office 9150 site in the RLC network.
Time Offset	Click the up or down arrows to change the time zone difference between this Remote Office 9150 unit and the RLC. Note: Time Offset is in 15-minute intervals to a maximum of, plus or minus, 24 hours.
Emergency Activation Code	If you are using the PSTN to route calls, then enter the number your community dials to reach an emergency service. Note: Only enter the Emergency Activation Code (for example, 911 in North America). Do not include the trunk access code because the Emergency Activation code dials out directly on the PSTN. If you are using only the IP network to route calls, leave this field blank.

Field	Description
SPRE Codes: Online	Enter the SPRE code that is used to put your site into online mode, or accept the default. The default is #99. Note: The SPRE code is automatically prefixed with the pound sign (# in North America). This means users must dial # before the SPRE code when going into online mode. Maximum length: 3 digits in addition to the pound sign. Refer to "Online/offline table" on page 46 for more information.
SPRE Codes: Paging	Enter the SPRE code that is used to announce pages to other stations in your office, or accept the default code. The default is #05. Note: The SPRE code is automatically prefixed with a pound sign (#). This means users must dial # before the SPRE code when initiating a page. Maximum length: 3 digits in addition to the pound sign
SPRE Codes: Registration	Enter the SPRE code that allows a multi-user or port-sharing participant to begin a session, or accept the default code. The default is #97. Note: The SPRE code is automatically prefixed with a pound sign (#). This means users must dial # before the SPRE code when registering for a port. Maximum length: 3 digits in addition to the pound sign
SPRE Codes: Offline	Enter the SPRE code that is used to put your site into offline mode, or accept the default code. The default is #98. Note: The SPRE code is automatically prefixed with the pound sign (# in North America). This means users must dial # before the SPRE code when going into offline mode. Maximum length: 3 digits in addition to the pound sign

Field	Description
SPRE Codes: Local Calling	Enter the SPRE code that allows analog or ATA-equipped station users to change the outgoing call mode to locally controlled mode. The default is #8. Note: The SPRE code is automatically prefixed with a pound sign (#). This means users must dial # before the SPRE code when initiating a local call on an analog or ATA-equipped station. Maximum length: 3 digits in addition to the pound sign
SPRE Codes: DeRegistration	Enter the SPRE code that will allow a multi-user or port sharing participant to end a session, or accept the default code. The default is #96. Note: The SPRE code is automatically prefixed with a pound sign (#). This means users must dial # before the SPRE code when disengaging from a port. Maximum length: 3 digits in addition to the pound sign
Trunk support	Choose 56K if you know that your Remote Office 9150 unit is in a PSTN network that can only transport at 56K. Choose 64K if you know that your Remote Office 9150 unit is in a PSTN network that supports speeds that vary from 64K to 56K. The Remote Office system dynamically adapts and downgrades a call to 56K if 64K is not available.

Field	Description
Local SwitchOver	Select Enable to automatically route through the Remote Office 9150 unit, the voice path for local station-to-station calls that are made on the host call appearance key. The signaling data is routed through the host PBX. However, the voice path is routed through the Remote Office 9150 unit to: ■ prevent tromboning between the RLC and Remote Office 9150 unit ■ save connection bandwidth Select Disable to route the voice path through the PBX. Note: You must enable the DN Discovery feature in order for the Local SwitchOver feature to work. Refer to the <i>Reach Line Card Installation and Administration Guide</i> (NTP 555-8421-210) to enable DN Discovery.
Companding Algorithm	Select the companding algorithm for the Remote Office 9150 unit. Valid options are: Mu-law, A-law, Automatic Note: A-law is standard for Europe and most areas outside of North America. Mu-law is standard for Japan and North America.
Multiple Subscriber Number	Choose Enable if the Central Office has given a separate DN number to each B-channel. Choose Disable if the Central Office has given a separate DN number to each B-channel.

Configuring International Tones

The Tone Code field on the International Tones Support dialog box specifies the frequency and levels for the NT8D17 TDS card.

When configuring International Tones, consider the following:

- International Tone configuration uses NT8D17 card Tone Codes. These codes are valid for all countries and Option11/IPE Controller cards.
- To configure the four international tones, you need to obtain the following FTC values for DIAL, RGBK, BUSY and OVFL from LD 56 of your PBX:

```
>ld 56
REQ prt
TYPE FTC      Look for the DIAL, RGBK, BUSY and OVFL values
...
DIAL
XTON 129      Enter the XTON value as the "Tone Code" value for this tone
XCAD 000      XCAD is used below to determine the Repeat, No. of Cycles and Cadence Time
RGBK
XTON 132
XCAD 32
BUSY
XTON 130
XCAD 30
OVFL
XTON 130
XCAD 0
```


In the following example there are three different values for XCAD. Collect the LD 56 WCAD details for each different XCAD value.

```
>ld 56
REQ prt
TYPE FCAD
WCAD 0      for XCAD 0
CDNC 00000 00000 00000 00000 00000 00000 00000 0000 00000
END OFF
WTON NO
```

```
REQ prt
WCAD 30
CDNC 100 50 00000 ...
END REPT
CYCS 1
WTON NO
```

```
REQ prt
WCAD 32
CDNC 102 102 205 819 00000 ...
END REPT
CYCS 1 2
WTON NO
```

Note the values printed for CDNC, END, and CYCS.

If END = REPT, then the value entered into the End Repeat field is "Repeat". CYCS usually has "1" or "1 2". Enter the largest number as the No. of Cycles. Enter the non-zero CDNC values into the Cadence Time fields.

Getting there 9150 → Configuration Manager → 9150 System Configuration

International Tones Support property sheet

The screenshot shows a dialog box titled "International Tones Support". It contains the following fields and controls:

- Tone Type:** A dropdown menu currently set to "DIAL".
- End Repeat:** Two radio buttons, "Off" (selected) and "Repeat".
- Tone Code:** A text input field containing the number "4".
- No of Cycles:** A text input field containing the number "0".
- Cadence Time:** A section containing eight small, empty rectangular input boxes arranged in two rows of four.
- Buttons:** Four buttons at the bottom: "OK", "Close", "Default", and "Help".

To configure International Tones

- 1 Click on the International Tones button in the System Configuration sheet.
- 2 Complete the fields as described in "International Tone field descriptions" on page 193.
- 3 Click OK to save the information in the temporary work file.

International Tone field descriptions

Field	Description
Tone Type	Enter the Tone Type for your country. Valid options are: Dial, RGBK, BUSY, OVFL Dial: dial tone signifies that the telephone is ready to receive dialed digits. RGBK: ringback signifies that the dialed line is ringing. Busy: busy signal signifies that the dialed line is not ready to receive calls. Ovfl: overflow (congestion) tone signifies that there are no channels available.
End Repeat	Select Off if you want the tone type you selected to be a constant tone. Select Repeat if you want the selected tone type to have on and off phases. Note: If you chose End Repeat: Off, then the No of Cycles and Cadence Time fields are dimmed.
Tone Code	Enter the four letter LD 56 Tone Codes that you want this Remote Office 9150 unit to use for the tone type you selected.
No of Cycles	Enter the number of cycles that you want in the tone type you selected. Two boxes in the Cadence Time field become active for each cycle you request. Valid options are: 1, 2, 3, 4
Cadence Time	Enter the length, in milliseconds, of the phases of the cadence that you want to configure for the tone type you selected. Refer to the <i>X11 Administration Guide</i> (NTP 553-3001-311) for more information.

Note: Refer to the Configuration Manager Help file for more information about International Tones.

Configuring the Remote Office 9150 unit's IP interface

This section explains how to enter the IP address, subnet mask, and default gateway for the Remote Office 9150 unit.

Differentiated Services (DiffServ)

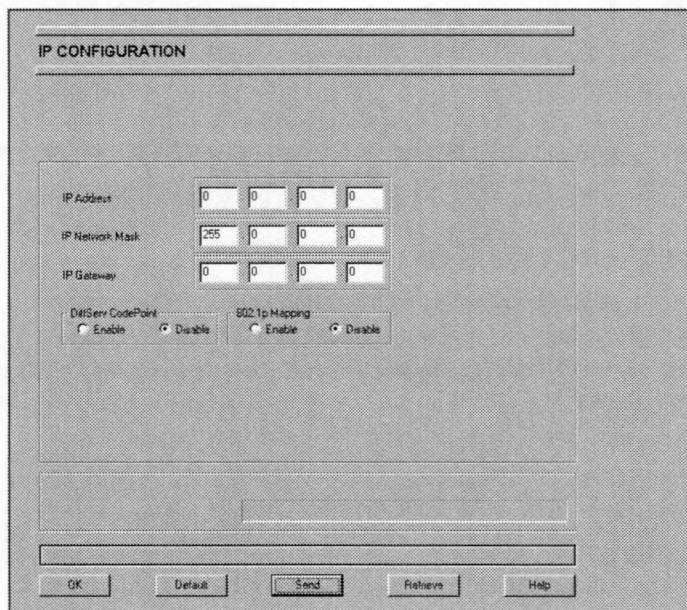
This setting modifies the IP Header and is applicable across the entire WAN. If enabled, this feature allows the Remote Office 9150 unit to set the DiffServ code-point to Nortel Network's standards for Voice over IP: EF (Expedited Forwarding).

802.1p

This setting inserts an additional tag at the Media Access Control (MAC) layer of IEEE 802.3 and therefore ends at the first router. Refer to RFC 2474.

Getting there 9150 → Configuration Manager → IP Configuration

IP Configuration sheet



The image shows a software dialog box titled "IP CONFIGURATION". It contains several input fields and radio buttons. The "IP Address" field has four boxes, each containing the digit "0". The "IP Network Mask" field has four boxes, with the first containing "255" and the others "0". The "IP Gateway" field has four boxes, each containing the digit "0". Below these are two sections: "DiffServ CodePoint" with "Enable" and "Disable" radio buttons (the latter is selected), and "802.1p Mapping" with "Enable" and "Disable" radio buttons (the latter is selected). At the bottom of the dialog are five buttons: "OK", "Default", "Send", "Retrieve", and "Help".

To enter the IP addresses

- 1 Enter the IP address assigned to the Remote Office 9150 unit into the IP Address boxes.
- 2 Enter the subnet mask into the IP Network Mask boxes.
- 3 Enter the IP address of the network gateway into the IP Gateway boxes.
- 4 To enable DiffServ, click on the **Enable** option button in the DiffServ CodePoint field.
- 5 To enable 802.1p mapping, click on the **Enable** button in the 802.1p Mapping field.
- 6 Click OK to save the information in the temporary work file.

- 7 To update the Remote Office 9150 unit with the new information, click Send.

IF you are

THEN

logged on to the Remote Office 9150 unit

the changes are written into the Remote Office 9150 unit's buffer.

To save the changes in flash memory, choose Upload/Download → Save to Flash.

not logged on to the Remote Office 9150 unit

The Connection not Established dialog box appears.

Do one of the following:

- Log on to the Remote Office 9150 unit, and then click Send again.
 - Save the changes to a file on your administration PC.
-

- 8 Restart the Remote Office 9150 unit.

Note: For instructions on how to restart the Remote Office 9150 unit, see "Performing a system restart or shutdown" on page 177.

Configuring the RLC connection information

This section describes how to configure information needed by the Remote Office 9150 unit to establish connections with the RLC on the host PBX.

Getting there 9150 → Configuration Manager → RLC Connection Configuration

RLC Connection Configuration sheet

RLC CONNECTION CONFIGURATION

Unit ID:

IP Connection: ☐ Enable ☐ Disable

IP Address:

IP Signaling: ☐ No Security ☐ Secure

Security Level:

Caller ID:

PSTN Connection: ☐ Enable ☐ Disable

PSTN Number to Connect to RLC:

Block Incoming Local Call on Primary S Channel: ☐ Enable ☐ Disable

Security Id:

Inbound Security ID:

Outbound Security ID:

OK Default Send Retrieve Help

To configure the RLC connection information

- 1 Complete the fields as described in "RLC Connection Configuration field descriptions" on page 200.
- 2 Click OK to save the information in the temporary work file.
- 3 To update the Remote Office 9150 unit with the new information, click Send.

IF you are

THEN

logged on to the
Remote Office 9150 unit

the changes are written into the Remote
Office 9150 unit's buffer.

To save the changes in flash memory, choose
Upload/Download → Save to Flash.

not logged on to the
Remote Office 9150 unit

The Connection not Established dialog box
appears.

Do one of the following:

- Log on to the Remote Office 9150 unit,
and then click Send again.
 - Save the changes to a file on your
administration PC.
-

RLC Connection Configuration field descriptions

Field	Description
Unit ID	Enter the number (between 1 and 255) assigned to the RLC to which this Remote Office 9150 unit is connected. The RLC's unit ID must be different from ■ this Remote Office 9150 unit's ID ■ the IDs of other units that are also connected to the RLC Note: This Unit ID must be entered on the Remote Connection Configuration property sheet on the RLC to create the communication path between this Remote Office 9150 unit and the RLC.
IP Connection	Select Enable if you want to route calls over your IP network. Select Disable if you do not want to route calls over your IP network.
IP Address	Enter the RLC's IP address. The Remote Office 9150 unit will use this IP address to connect to the RLC over the IP network.
IP Signaling	Select Enable if you want to set the IP signaling connection to permanent mode on the Remote Office 9150 unit. Refer to "Deployment options" on page 82 for more information.
PSTN Connection	Select Enable if you want to route calls over the PSTN. Select Disable if you do not want to route calls over the PSTN.

Field	Description
Block Incoming Local Call on Primary B Channel	Select Enable if incoming local calls <i>should not</i> be received on the first B-channel. Select Disable if the first B-channel <i>should</i> receive incoming local calls.

Configuring the PSTN connection number

The PSTN number corresponds to the dedicated network port on the RLC for your Remote Office 9150 unit. The PSTN number to connect to the RLC must be configured in a specific manner. If you select Caller ID as the security level, then the PSTN number that you enter for the Remote Office 9150 unit to connect to the RLC is compared with the telephone number configured on the RLC for your site. If the two numbers do not match, the call is dropped.

Note: Enter the PSTN number to connect to RLC exactly as it must be dialed by the Remote Office 9150 unit, including 1 for long distance and 9 for Centrex trunk access.

Getting there 9150 → Configuration Manager → RLC Connection Configuration

RLC Connection Configuration sheet

RLC CONNECTION CONFIGURATION

Unit ID

254

IP Connection

Enable

Disable

IP Address

IP Signaling

Relay

Direct

Security Level

Security Level

No Security

Caller ID

PSTN Connection

Enable

Disable

PSTN Number to Connect to RLC

Block Incoming Local Call on Primary B Channel

Enable

Disable

Security ID

Inbound Security ID

Outbound Security ID

OK

Default

Send

Retrieve

Help

To configure the PSTN number

- 1 Enable the PSTN Connection option.
- 2 Enter the telephone that the Remote Office 9150 unit will dial to connect to the RLC in the PSTN Number to Connect to RLC field.
- 3 Click OK to save the information in the temporary work file.
- 4 To update the Remote Office 9150 unit with the new information, click Send.

IF you are

THEN

logged on to the
Remote Office 9150 unit

the changes are written into the Remote
Office 9150 unit's buffer.

To save the changes in flash memory, choose
Upload/Download → Save to Flash.

not logged on to the
Remote Office 9150 unit

The Connection not Established dialog box
appears.

Do one of the following:

- Log on to the Remote Office 9150 unit,
and then click Send again.
 - Save the changes to a file on your
administration PC.
-

Configuring the security level

It is recommended that you implement a security authentication method on both the RLC and the Remote Office 9150 unit to prevent toll fraud.

The security level defines what type of security authentication is used between the Remote Office 9150 unit and the host PBX. The information used to perform security authentication depends on the security level chosen. There are three levels of security:

- No security (default setting)
- Caller ID
- Provision ID

For a detailed description of these security levels refer to “System security” on page 30.

Getting there 9150 → Configuration Manager → RLC Connection Configuration

RLC Connection Configuration sheet

RLC CONNECTION CONFIGURATION

Unit ID: 254

IP Connection: ☐ Enable ☒ Disable

IP Address: [][][][]

IP Signaling: ☒ Provisioned ☐ On Demand

PSTN Connection: ☐ Enable ☒ Disable

PSTN Number to Connect to RLC: []

Block Incoming Local Call on Primary B Channel: ☒ Enable ☐ Disable

Security Level: No Security

Security Id: Inbound Security ID: [] Outbound Security ID: []

Caller ID: []

OK Default Send Retrieve Help

To configure the security level

- 1 Select one of the following security level settings from the Security Level list box:
 - No Security
 - Caller ID
 - Provision ID

- 2 If you selected Caller ID or Provision ID security levels, do one of the following:

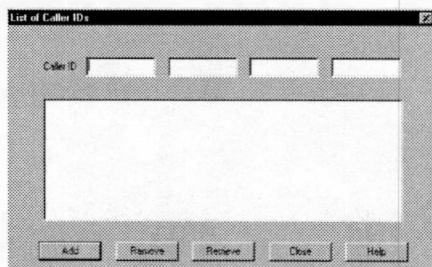
IF you selected

THEN

Caller ID

click CallerID.

Result: The List of Caller IDs dialog box appears.



In the Caller ID box, enter the telephone number from which the Remote Office 9150 unit can accept calls. Ensure that the telephone number you enter matches the Caller ID actually presented by the RLC.

Click OK, and then click Add from the pop-up menu that appears.

Result: The telephone number appears in the blank box.

IF you selected	THEN
Provision ID	the Security ID fields are enabled. Do the following: ■ Enter the RLC's security identifier (must be a 10 digit password) in the Inbound Security ID field. ■ Enter the Remote Office 9150 unit's security identifier (must be a 10 digit password) in the Outbound Security ID field. Note: You must configure the same security identifiers in reverse on the RLC port to which this Remote Office 9150 unit is assigned.

- 3 Click OK to save the information in the temporary work file.
- 4 To update the Remote Office 9150 unit with the new information, click Send.

IF you are	THEN
logged on to the Remote Office 9150 unit	the changes are written into the Remote Office 9150 unit's buffer. To save the changes in flash memory, choose Upload/Download → Save to Flash.
not logged on to the Remote Office 9150 unit	The Connection not Established dialog box appears. Do one of the following: ■ Log on to the Remote Office 9150 unit, and then click Send again. ■ Save the changes to a file on your administration PC.

Configuring trunks and trunk groups

This section explains how to configure your trunks to connect with the RLC at the host site, or to make calls through the local PSTN. The procedure to configure BRI trunks can be found on page 211. The procedure to configure trunk groups can be found on page 215.

Trunks

A trunk is the straight connection between the PSTN and the Remote Office 9150 unit. Each ISDN BRI line (up to four are supported by the Remote Office 9150 unit) provides two B-channels. In Remote Office 9150 unit context, each B-channel equals one trunk.

Each B-channel can be defined as a local trunk, remote trunk, or both.

Note: Remote Office 9150 units support MSN. If each B-channel has a unique DN then the configuration of the first B-channel defines both b-channels.

Local trunk

The trunk is used to make local calls over the PSTN.

Remote trunk

A remote trunk is used to establish a connection to the RLC from the Remote Office 9150 unit.

Local and remote trunk

A B-channel that is defined as both local and remote can be used to make calls through both the local PSTN, as well as through the RLC on the host PBX.

Primary trunk on the Remote Office 9150 unit

The primary trunk on the Remote Office 9150 unit is one of the following:

- the lowest-numbered B-channel defined as Remote only
- the lowest-numbered B-channel defined as Local and Remote

Since a local call can cause blocking of an incoming host-controlled call on a B-channel defined as Local and Remote, or prevent QoS transitions from occurring, Nortel Networks recommends that you configure the primary trunk as Remote only. For example, Module 4 first B channel.

Do not include the primary trunk in any trunk groups.

Trunk groups

A trunk group consists of one or more B-channels that are logically grouped. You can configure up to eight trunk groups. For example, you can configure

- each B-channel as a different trunk group
- two or more B-channels as a trunk group

A B-channel can be a member of more than one trunk group.

Trunk access codes

Trunk access codes are numbers that are used by the Remote Office 9150 unit to determine which trunk group to use when routing the call. You must define a trunk access code for each trunk group.

For example, you can assign trunk access codes #61 and #62, as shown below:

Group 1	Group 2
Trunk 1	Trunk 3
Trunk 2	Trunk 4
Trunk access code: #61	Trunk access code: #62

If a user dials trunk access code #61, the call is routed (or processed) using trunks 1 or 2. If trunks 1 and 2 are both busy, the user's call is blocked (the user receives a fast busy signal).

Note: All trunk access codes are automatically defined in Configuration Manager with a pound prefix (# in North America) so that there are no conflicts with host PBX dialing plans. Trunk access codes must be between one and three digits in length in addition to the pound sign.

For a list of the default trunk access codes, refer to the “Remote Office 9150 Configuration Information—Dialing Plans on page 354.

ISDN configuration

In order to configure European ISDN, the PSTN must support the following features:

- Multiple Subscriber Numbering (MSN)
- Two directory numbers (one per B channel)

The default configuration setting for BRI SPIDs is NC (Not Configured). Ensure that no supplemental ISDN services, (for example, Call Waiting) are provided as this may disrupt the data path and drop calls.

European ISDN

When configuring EuroISDN and ETSI variants, the BRI Configuration SPIDs must be set to NC (not configured).

To change EuroISDN SPID values, complete the following procedure:

- 1 Go to Configuration Manager > 9150 > BRI Configuration.
- 2 Click on the **Default** button.
- 3 Configure the DNs, SPIDs, and ISDN line type.

Note: Only A-Law configuration is fully supported with ETSI configurations.

National ISDN

If you select National ISDN as the line type, there are minor protocol differences between National ISDN -1, -2, -3, and -4. The Proprietary Switch line type is more general and should be used if problems are encountered.

Configuring BRI trunks

This topic shows you how to configure the BRI trunks. See “Configuring trunks and trunk groups” on page 208 for a detailed explanation of BRI configuration settings.

Getting there 9150 → Configuration Manager → BRI Configuration

BRI Configuration sheet

The image shows a screenshot of the "BRI CONFIGURATION" window. The window has a title bar and a menu bar. Below the menu bar, there are several sections for configuration:

- Module #**: A dropdown menu showing "1".
- ISDN Line Type**: A dropdown menu showing "Proprietary Switch".
- Switch Type**: A dropdown menu showing "Unknown".
- B Channel 1**:
 - Status**: Radio buttons for "Enable" and "Disable". "Disable" is selected.
 - Type**: Radio buttons for "Local", "Remote", and "Local & Remote". "Local & Remote" is selected.
 - PSTN Number**: A text field containing "NC".
 - SPID**: A text field containing "NC".
- B Channel 2**:
 - Status**: Radio buttons for "Enable" and "Disable". "Disable" is selected.
 - Type**: Radio buttons for "Local", "Remote", and "Local & Remote". "Local & Remote" is selected.
 - PSTN Number**: A text field containing "NC".
 - SPID**: A text field containing "NC".

At the bottom of the window, there are five buttons: "OK", "Default", "Send", "Retrieve", and "Help".

To enter the BRI settings

- 1 Complete the fields as described in "BRI Configuration field descriptions" on page 213.
- 2 Click OK to save the information in the temporary work file.
- 3 To update the Remote Office 9150 unit with the new information, click Send.

IF you are	THEN
logged on to the Remote Office 9150 unit	the changes are written into the Remote Office 9150 unit's buffer. To save the changes in flash memory, choose Upload/Download → Save to Flash.
not logged on to the Remote Office 9150 unit	The Connection not Established dialog box appears. Do one of the following: ■ Log on to the Remote Office 9150 unit, and then click Send again. ■ Save the changes to a file on your administration PC.

BRI Configuration field descriptions

Field	Description
Module #	Select the number identifying the trunk interface module that you are configuring. Note: The number you select must match the module position where the module has been installed. Valid options: 4 through 7
ISDN Line Type	Select the ISDN variant used in your country. Get this information from your ISDN service provider.
Switch Type	Select the type of switch used by your ISDN service provider for this trunk. Get this information from your ISDN service provider.
Status (B channel 1 and B channel 2)	Select Enable to activate the ISDN BRI channel. Select Disable to deactivate it.
Type (B channel 1 and B channel 2)	Select the type of connection—local, remote, or local and remote. ■ Local: This trunk is used for local PSTN calls only. ■ Remote: This trunk creates a circuit-switched connection path to the host PBX. ■ Local & Remote: This trunk can route local PSTN calls and host PBX calls. Note: If you select Local or Local & Remote, then the Allocation field is enabled.

Field	Description
PSTN Number (B channel 1 and B channel 2)	Enter the full telephone number provided to you by your ISDN service provider for this B-channel. Include access codes, dialing prefix, and area code if necessary. When entering the area code, always enter it directly before the main telephone number. Do not use a hyphen (-) as a separator because hyphens are reserved for subaddressing.
SPID (B channel 1 and B channel 2)	Enter the Service Profile Identifier (SPID) provided to you by your ISDN service provider for this B-channel.

Configuring trunk groups

This section shows you how to enable and create trunk groups for use with the Remote Office 9150 unit. For more information, see “Trunk groups” and “Trunk access codes” on page 209.

Getting there 9150 → Configuration Manager → Trunk Group Configuration

Trunk Group Configuration sheet

The screenshot shows a dialog box titled "TRUNK GROUP CONFIGURATION". It contains the following fields and controls:

- Trunk Groups** section:
 - Group No**: A dropdown menu with "1" selected.
 - Status**: Two radio buttons, "Enable" (selected) and "Disable".
 - Trunk Access Code**: A text field containing "61".
 - Local DNs to Alert**: A section with a checked checkbox labeled "Not Configured" and five empty text input fields below it.
 - Trunk Group B Channels**: A button.
- At the bottom, there are five buttons: "OK", "Default", "Send", "Retrieve", and "Help".

To configure trunk groups

- 1 Complete the fields as described in “Trunk Group Configuration field descriptions” below.
- 2 Click OK to save the information in the temporary work file.

- 3 To update the Remote Office 9150 unit with the new information, click Send.

IF you are	THEN
logged on to the Remote Office 9150 unit	the changes are written into the Remote Office 9150 unit's buffer. To save the changes in flash memory, choose Upload/Download → Save to Flash.
not logged on to the Remote Office 9150 unit	The Connection not Established dialog box appears. Do one of the following: ■ Log on to the Remote Office 9150 unit, and then click Send again. ■ Save the changes to a file on your administration PC.

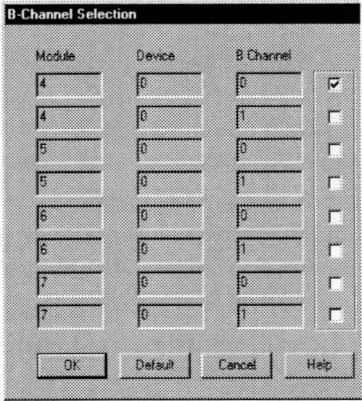
Trunk Group Configuration field descriptions

Field	Description
Group No	Select a group number. You can create up to ten groups.
Status	Select Enable to activate the trunk group. Select Disable to deactivate the trunk group.
Trunk Access Code	Enter the trunk access code that you want to assign to the trunk group, or accept the default. Note: The trunk access code is automatically prefixed with a pound sign (# in North America). This means users must dial the # before the trunk access code when making an outgoing local call. Maximum length: 1 to 3 digits in addition to the pound sign
Local DNs to Alert: Not Configured	Select the Not Configured box if you want all sets to ring for incoming local calls. If you want incoming calls to ring on specific telephones only, then enter the DNs of those telephones. If you do not configure DNs for a particular trunk group then all of the DNs (both Local only and Local and Remote) will alert. If you configure DNs but the trunk group is disabled, then all of the DNs (both Local only and Local and Remote) will alert.

Field	Description
-------	-------------

Trunk Group
B Channels

Click Trunk Group B Channels.
Result: The Trunk Group B-Channel dialog box appears.



The B-Channel Selection dialog box contains a table with four columns: Module, Device, B Channel, and a checkbox. The table lists 8 rows of data. The first row has Module 4, Device 0, B Channel 0, and the checkbox is checked. The remaining 7 rows have Module 4, 5, 6, 6, 7, 7 and Device 0, with B Channels 1, 0, 1, 0, 0, 1 respectively, and all checkboxes are unchecked. At the bottom are buttons for OK, Default, Cancel, and Help.

Module	Device	B Channel	
4	0	0	☒
4	0	1	☐
5	0	0	☐
5	0	1	☐
6	0	0	☐
6	0	1	☐
7	0	0	☐
7	0	1	☐

OK Default Cancel Help

Trunk Group
B Channels
(continued)

- Complete the fields as follows:
- **Module:** Displays trunk interface module numbers.
 - **Device:** Displays the internal device number for each B-channel provided by the module.
 - **B Channel:** Displays B-channel numbers.
 - **Check boxes:** Click the check box for each B-channel you want to include in this trunk group.

Note: A B-channel can be a member of more than one trunk group.

Click OK.

Configuring stations

This section explains how to configure the Remote Office 9150 unit so that it can:

- route calls between the stations at your site and the host PBX
Each station is associated with a port on the RLC, and can be configured with different capabilities.
- make calls through the local PSTN or to other stations at the Remote Office 9150 site

If resources on the RLC on the host PBX allow, you can configure up to 32 telephone stations plus one analog device (such as an analog telephone or fax machine). This configuration assumes that none of the stations are equipped with Analog Telephone Adapters (ATAs) or Meridian Communication Adapters (MCAs).

Bridge Ports

Bridge Ports are proxy ports that represent local calls or inbound PSTN calls to the PBX. When a local call on a Remote Office 9150 unit needs PBX services, the Bridge Port obtains a PBX presence on behalf of the local call.

When configuring Bridge Ports:

- Consider the number of simultaneous remote service telephone calls and the number of bridge ports in use when determining PSTN or IP bandwidth needs.
- Remember that every local ISDN call reduces the PSTN bandwidth available for remote service telephone calls and bridge ports when determining needed PSTN bandwidth.

Notes: You can configure a maximum of sixteen (16) Bridge Ports. You must configure at least one SCR key on the set for the Bridge Port feature to work.

You must configure Bridge Port parameters on both the RLC and Remote Office 9150 unit. For information regarding Bridge Port configuration on the RLC, refer to the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210).

Note: Local Only sets do not support conference calls to a local Remote Office 9150 unit or to a host PBX. Local Only sets can dial host PBX DN's using an enabled Bridge Port.

Configuring Bridge Ports reduces the total number of ports available from the RLC.

Call processing capabilities and station settings

Each station can be defined as a telephone that can process

- local calls only
- remote calls only
- local and remote calls

Stations defined with local call capability are further defined with telephone features and local call appearance keys. Stations that are defined with remote call capability do not need to be further configured because they inherit their features and call appearance keys from their associated port configurations on the host PBX.

Local call capability

Stations defined as *local* can make and receive calls through the local PSTN or to other stations at the Remote Office 9150 site. Calls through the host PBX are not allowed.

Local stations are not associated with RLC ports.

Remote call capability

Stations defined as *remote* are associated with RLC ports, and can make and receive calls through the host PBX only. Calls through the local PSTN are not allowed.

Local and remote call capability

Stations defined as *local and remote* are associated with RLC ports, and can

- make and receive calls through both the host PBX and the local PSTN
- make calls to other stations at the Remote Office 9150 site

Outgoing calls are routed according to the call appearance key used to initiate the call.

- Calls initiated on the key defined as the host call appearance key (also referred to as the *primary DN key*) are routed through the host PBX.
- External calls initiated on the key defined as the local call appearance key are routed through the local PSTN.
- Internal calls initiated on the local call appearance key are routed to other stations at the Remote Office 9150 site.

The Remote Office 9150 unit distinguishes an incoming call by its calling line identification, and rings it as follows:

- on the host call appearance key if the call was routed through the host PBX
- on the local call appearance key if the call was routed through the local PSTN or if the call was a station-to-station call

Local station settings

When a station is defined with local capability, you can further configure the station to

- enable or disable certain features (for more details, see “Defining stations” on page 225)
- disable outgoing dialing digit sequences (see “Disabled Outbound Digit Sequence” on page 229)
- identify local call appearance and feature key positions (see “Optional Feature Keys” on page 230)

Remote station settings

When the station is defined with remote capability, you can assign it to a specific port on the RLC (see “Defining stations” on page 225).

Call appearance keys

The host call appearance key is defined for each station on the host PBX. It is not defined for each station on the Remote Office 9150 unit.

The local call appearance keys, on the other hand, must be defined for each station connected to the Remote Office 9150 unit to allow

- users to make outgoing calls using Remote Office 9150 trunks
- users to make station-to-station calls without host PBX control
- incoming calls on Remote Office 9150 trunks to ring specific stations

The local call appearance keys must be left undefined in the host PBX configuration to avoid indicator conflicts between the host PBX and the Remote Office 9150 unit. Only indicators defined as local call appearances are blocked from the host PBX.

When to configure the local call appearance keys

The local call appearance key positions must be defined when a new station is being configured with local capability, or when a request to change feature key positions has been initiated.

Associating trunk groups with local stations

Each trunk group can be defined to ring only specific stations. This feature allows you to route certain types of calls (such as incoming calls on a 1-800 number) to specific stations.

Private lines

A private line is a telephone line that is used by one person only. Calls that are routed to the private line do not ring on any other station in your office. To dedicate a private line to a station, configure a trunk group to ring incoming calls only on that station.

If you are connecting a fax machine to the Remote Office 9150 unit, then configure a private line to the fax. Incoming calls on this line are routed directly to the fax.

For instructions, refer to “Configuring trunk groups” on page 215.

Calling permissions and restrictions

You can consider the ability to make certain types of calls from a station to be a calling permission. Similarly, a certain type of call that is not allowed is a calling restriction.

You can define both permissions and restrictions for each station.

Local and remote calling permissions

When you define a station as a local station, you are granting the station with local calling permission. Calls can be made or received through the local PSTN or to and from other stations. Calls through the host PBX are not allowed.

When you define a station as a remote station, you are granting the station with remote calling permission. Calls can be made or received through the host PBX only. Calls through the local PSTN are not allowed.

Exception: If the emergency service number is configured on the Remote Office 9150 unit and you are using the PSTN to route calls, the dialed emergency service number is routed through the local PSTN to the emergency service. This ensures that the emergency service receives the correct calling location information.

When you define a station as a local and remote station, you are granting the station with the ability to make or receive calls through both the local PSTN and the host PBX. Station-to-station calls are also allowed.

Call restriction

You can prevent certain types of calls from being made at a station by disabling the digits that normally allow the call to proceed. This option is available for stations designated as Local or both Local and Remote.

For example, if you want to prevent someone from calling a 1-976 number, enter 976 as the digits to disable. For more information refer to "Disabled Outbound Digit Sequence" on page 229, in the Local Profile Configuration field description section.

ATA- and MCA-equipped stations and bandwidth requirements

Each station equipped with an MCA requires a full 64 Kbps of bandwidth to the host PBX.

For stations equipped with ATA devices, the bandwidth used by calls processed on those stations is as follows:

IF	THEN
G.729 compression is being used and the call is a voice call	the voice call is sent as 8 Kbps to the host PBX.
G.729/Fax or G.711 compression is being used and the call is a fax call	the fax call is sent as 64 Kbps.
the call is a local call	the voice call is not compressed. It is sent as 64 Kbps of data across the ISDN BRI B-channel.

The following table identifies the number of MCAs or ATAs that can be connected to the Remote Office 9150 unit:

IF the Remote Office 9150 unit is connected to	THEN you can connect
a 1-slot RLC (supporting 16 users)	four MCAs or ATAs to the Remote Office 9150 unit.
a 2-slot RLC (supporting 32 users)	seven MCAs or ATAs to the Remote Office 9150 unit.

Notes:

- You can have eight MCAs or ATAs installed if an analog telephone or fax machine is *not* installed.
- The total number of digital telephones and ATAs cannot exceed 32.

Defining stations

To make and receive calls, you must use Configuration Manager to configure each station (telephone or other device such as a fax machine) in your office.

Note: To ensure that digital telephones, ATAs, and MCAs operate as expected, you must specify the Phone Type when configuring a station as Local or Remote.

Getting there 9150 → Configuration Manager → 9150 Port Configuration

9150 Port Configuration sheet

The screenshot shows the '9150 PORT CONFIGURATION' window. At the top, there are tabs for 'Ports 0 - 15', 'Ports 16 - 31', 'Ports 32 - 47', and 'Ports 48 - 64'. The 'Ports 0 - 15' tab is selected. Below the tabs, there is a table with columns for 'Port Type', 'RLC Port', and 'Description'. Each row represents a port from 0 to 15. The 'Port Type' column has three radio buttons: 'Local', 'Remote', and 'Local & Remote'. The 'RLC Port' column has a numeric input field. The 'Description' column has a text field with the text 'Autohold Enabled, Paging Enabled, C'. To the right of each row is a 'Configure' button. At the bottom of the window, there are buttons for 'OK', 'Default', 'Send', 'Retrieve', 'Get DN List', and 'Help'.

Port	Port Type	RLC Port	Description	Configure
0	☒ Local ☐ Remote ☐ Local & Remote	0	Autohold Enabled, Paging Enabled, C	Configure
1	☒ Local ☐ Remote ☐ Local & Remote	1	Autohold Enabled, Paging Enabled, C	Configure
2	☒ Local ☐ Remote ☐ Local & Remote	2	Autohold Enabled, Paging Enabled, C	Configure
3	☒ Local ☐ Remote ☐ Local & Remote	3	Autohold Enabled, Paging Enabled, C	Configure
4	☒ Local ☐ Remote ☐ Local & Remote	4	Autohold Enabled, Paging Enabled, C	Configure
5	☒ Local ☐ Remote ☐ Local & Remote	5	Autohold Enabled, Paging Enabled, C	Configure
6	☒ Local ☐ Remote ☐ Local & Remote	6	Autohold Enabled, Paging Enabled, C	Configure
7	☒ Local ☐ Remote ☐ Local & Remote	7	Autohold Enabled, Paging Enabled, C	Configure
8	☒ Local ☐ Remote ☐ Local & Remote	8	Autohold Enabled, Paging Enabled, C	Configure
9	☒ Local ☐ Remote ☐ Local & Remote	9	Autohold Enabled, Paging Enabled, C	Configure
10	☒ Local ☐ Remote ☐ Local & Remote	10	Autohold Enabled, Paging Enabled, C	Configure
11	☒ Local ☐ Remote ☐ Local & Remote	11	Autohold Enabled, Paging Enabled, C	Configure
12	☒ Local ☐ Remote ☐ Local & Remote	12	Autohold Enabled, Paging Enabled, C	Configure
13	☒ Local ☐ Remote ☐ Local & Remote	13	Autohold Enabled, Paging Enabled, C	Configure
14	☒ Local ☐ Remote ☐ Local & Remote	14	Autohold Enabled, Paging Enabled, C	Configure
15	☒ Local ☐ Remote ☐ Local & Remote	15	Autohold Enabled, Paging Enabled, C	Configure

Buttons at the bottom: OK, Default, Send, Retrieve, Get DN List, Help

To configure stations

- 1 Locate the port that you want to configure by clicking the appropriate port range tab, and then scrolling down the list.

The following table describes port number ranges and how they can be configured:

Ports	Can be assigned to
0–15 and 32–47	digital telephones. Note: The associated ports on the host PBX must be configured with voice capability.
16–31 and 48–63	stations equipped with ATAs or MCAs. Note: The associated ports on the host PBX must be configured with data capability.
64	a fax machine or other analog device (without an ATA). Note: The associated port on the host PBX must be configured with data capability.

Note: You can use ports 32–47 and 48–63 only if this Remote Office 9150 unit connects to a 2-slot RLC on the host PBX.

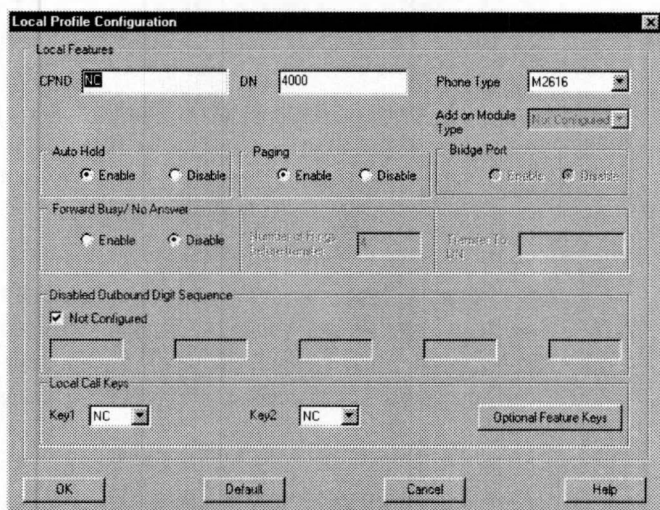
- 2 Under Port Type, click the call processing capability that this station should have:
 - Local: if only calls through the local PSTN are allowed. This option enables the Configure button for this port.
 - Remote: if only calls through the host PBX are allowed.
 - Local and Remote: if both local and remote calls and local station-to-station calling are allowed. This option enables the Configure button for this port so you can configure local station features and keys.
Note: Choose Local and Remote if you want to define a Bridge Port.
- 3 Accept the default RLC Port to which this station is assigned, or enter a new RLC port number.

Exception: Do not associate a local-only port with an RLC port.

Notes:

- Generally, the Remote Office 9150 port and RLC port should match to simplify configuration and administration.
 - If the station is equipped with an MCA or ATA for data transmission, or if the port is used for fax, the RLC port must be configured on the host PBX with data capability.
- 4 If you selected Local or Local & Remote, click Configure for the port you are configuring.

Result: The Local Profile Configuration property sheet appears.



The image shows a 'Local Profile Configuration' dialog box with the following fields and options:

- Local Features:**
 - CFND: DN: Phone Type:
 - Add on Module Type:
 - Auto Hold: ☒ Enable ☐ Disable
 - Paging: ☒ Enable ☐ Disable
 - Bridge Port: ☒ Enable ☐ Disable
 - Forward Busy/ No Answer: ☐ Enable ☒ Disable
 - Number of Rings Before Transfer: Transfer To DN:
 - Disabled Outbound Digit Sequence: ☒ Not Configured
 - Local Call Keys: Key1: Key2: Optional Feature Keys:

Buttons at the bottom: OK, Default, Cancel, Help.

- 5 Complete the fields as described in "Local Profile Configuration field descriptions" on page 228.
- 6 Once you have completed the Local Profile Configuration, click OK.

Result: The 9150 Device Configuration sheet reappears. The configurations you set are displayed in the port's Description box.

Local Profile Configuration field descriptions

Field	Description
CPND	Enter the calling party name display (CPND) for the user to which the station is assigned.
DN	Enter the user's local extension number. Note: If Auto DN Discovery is enabled on the RLC, then this field is configured to be the same DN as the primary DN configured on the host PBX for this station.
Phone Type	Select the telephone model type connected to the port. Valid options are: M2006, M2008, M2216, M2616, M2616CT, M3820, M3901, M3902, M3903, M3904, M3905, MCA, ATA, Other.
Add on Module Type	Select the applicable Add on Module for the M3904 and M3905 telephones. Valid options are: Not Configured, KBA, DBA.
Auto Hold	Select Enable if active calls should be automatically put on hold when another call appearance key is pressed. Select Disable if active calls should be disconnected when another call appearance key is pressed.
Paging	Select Enable if this station will be allowed to announce pages. Select Disable if this station will not be allowed to announce pages.
Bridge Port	Select Enable to inbound PSTN calls access to certain PBX features.
Forward Busy/No Answer	Select Enable to allow incoming calls to this station to be forwarded if they are not answered by the number of rings configured in the Number of Rings before transfer field or if the station is busy. Select Disable if calls should not be forwarded.

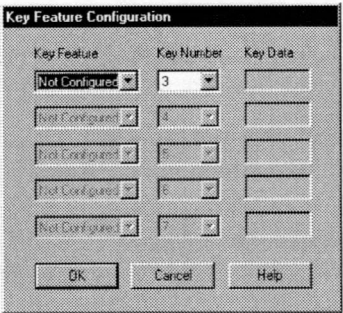
Field	Description
Forward Busy/No Answer: Number of Rings before transfer	Enter the number of times this station rings before transferring the call to the configured DN. Default is four rings.
Forward Busy/No Answer: Transfer to DN	Enter the DN where calls to this station will be transferred if not answered before the configured number of rings. This DN may be for a voicemail service or the DN of another station.
Disabled Outbound Digit Sequence	If you want to prevent this station from making a certain type of call, then enter the digits that normally allow that type of call to proceed. Example: Enter 1976 to prevent calls to 1-976 numbers. Note: You can configure five digit sequences. In order for calls to be restricted, the dialed number must contain a matching string at the beginning of the number.
Local Call Keys (Key 1 and Key 2)	The number selected identifies the feature key position on the telephone. Select the feature key you want to use for each local call appearance key. Valid options are: 1-15. NC means not configured. Note: If the port is configured as local and remote, Key 0 is not recommended. Keys 8 and 9 are recommended. You can select Key 0 if the port is configured as local only. Valid options: 0 through 15

Field	Description
-------	-------------

Optional Feature
Keys

If you configured the port as Local, click this button to assign local features to specific keys.

Result: The Key Feature Configuration property sheet appears.



Note: Ensure that the selected key does not already have a feature assigned to it through the PBX.

■ Key Feature

Select the name of the feature you want to configure on this key.

Valid options: Call Transfer, Call Forward, Auto Dial, Make Set Busy, Not Configured

■ Key Number:

The key number identifies the feature key position on the telephone. Select the key you want for the feature you are configuring.

Note: If the station is configured as local and remote, the key number selected for the feature must match the feature key position defined in the PBX voice port configuration.

Valid options: 0 through 15

■ Key Data

Enter the DN to be used by the feature, if applicable.

Configuring a fax station

The Remote Office 9150 unit provides the ability to connect and use a fax machine. You can define port 64 as the fax machine on the Remote Office 9150 unit in one of the following ways:

TO allow all fax calls to be made or received through	THEN
the local PSTN only	define the fax machine as a local device.
the host PBX	define the fax machine as a remote device.
both the local PSTN and the host PBX	define the fax machine as a local and remote device.

Note: When faxes are sent and received through the host PBX, they are sent uncompressed (that is, they require 64 Kbps of bandwidth).

For instructions on configuring the fax port, see “To configure the fax port” on page 232.

For instructions on configuring a trunk group that rings only on the fax machine, see “To configure trunk groups” on page 215.

Getting there 9150 → Configuration Manager → RLC Port Configuration

9150 Port Configuration sheet

Ports 0-15 | Ports 16-31 | Ports 32-47 | Ports 48-64

9150 PORT CONFIGURATION

Port	Port Type	RLC Port	Description	Configure
0	☒ Local ☐ Remote ☐ Local & Remote	0	Autohold Enabled Paging Enabled C	Configure
1	☒ Local ☐ Remote ☐ Local & Remote	1	Autohold Enabled Paging Enabled C	Configure
2	☒ Local ☐ Remote ☐ Local & Remote	2	Autohold Enabled Paging Enabled C	Configure
3	☒ Local ☐ Remote ☐ Local & Remote	3	Autohold Enabled Paging Enabled C	Configure
4	☒ Local ☐ Remote ☐ Local & Remote	4	Autohold Enabled Paging Enabled C	Configure
5	☒ Local ☐ Remote ☐ Local & Remote	5	Autohold Enabled Paging Enabled C	Configure
6	☒ Local ☐ Remote ☐ Local & Remote	6	Autohold Enabled Paging Enabled C	Configure
7	☒ Local ☐ Remote ☐ Local & Remote	7	Autohold Enabled Paging Enabled C	Configure
8	☒ Local ☐ Remote ☐ Local & Remote	8	Autohold Enabled Paging Enabled C	Configure
9	☒ Local ☐ Remote ☐ Local & Remote	9	Autohold Enabled Paging Enabled C	Configure
10	☒ Local ☐ Remote ☐ Local & Remote	10	Autohold Enabled Paging Enabled C	Configure
11	☒ Local ☐ Remote ☐ Local & Remote	11	Autohold Enabled Paging Enabled C	Configure
12	☒ Local ☐ Remote ☐ Local & Remote	12	Autohold Enabled Paging Enabled C	Configure
13	☒ Local ☐ Remote ☐ Local & Remote	13	Autohold Enabled Paging Enabled C	Configure
14	☒ Local ☐ Remote ☐ Local & Remote	14	Autohold Enabled Paging Enabled C	Configure
15	☒ Local ☐ Remote ☐ Local & Remote	15	Autohold Enabled Paging Enabled C	Configure

OF Default Send Retrieve Get DN List Help

To configure the fax port

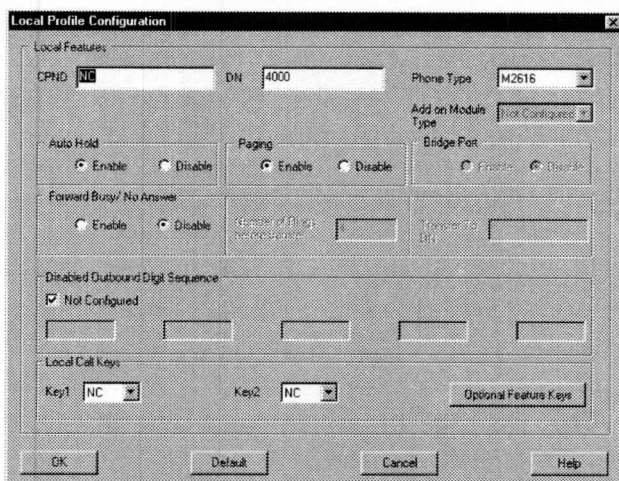
- 1 Locate port 64.
- 2 On port 64, under Port Type, click the call processing capability the fax machine should have:
 - Local: if only faxes through the local PSTN are allowed. This option enables the Configure button for this port.
 - Remote: if only faxes through the host PBX are allowed.
 - Local and Remote: if both local and remote faxing are allowed. This option enables the Configure button for this port so you can configure local station features and keys.

- 3 Accept the default RLC Port to which this station is assigned, or enter a new RLC port number.

Notes:

- Generally, the Remote Office 9150 port and RLC port should match to simplify configuration and administration.
 - For fax transmissions, the RLC port must be configured on the host PBX with data capability.
- 4 If you selected Local or Local & Remote, click Configure for the port you are configuring.

Result: The Local Profile Configuration dialog box appears.



The image shows a screenshot of the 'Local Profile Configuration' dialog box. The dialog has a title bar with 'Local Profile Configuration' and a close button. It contains several sections: 'Local Features' with fields for CPND (set to 'NC'), DN (set to '4000'), and Phone Type (set to 'M2516'); 'Auto Hold' with 'Enable' and 'Disable' radio buttons; 'Paging' with 'Enable' and 'Disable' radio buttons; 'Forward Busy/No Answer' with 'Enable' and 'Disable' radio buttons; 'Bridge Port' with 'Enable' and 'Disable' radio buttons; 'Disabled Outbound Digit Sequence' with a 'Not Configured' checkbox and five empty text boxes; 'Local Call Keys' with 'Key1' and 'Key2' dropdown menus (both set to 'NC') and an 'Optional Feature Keys' button. At the bottom are 'OK', 'Default', 'Cancel', and 'Help' buttons.

- 5 In the Local Features: CPND box, enter a description (for example, FAX).
- 6 Enter the number used to ring the fax machine in the Local Features: DN box.
- 7 Click Disable under Local Features for the following:
 - Auto Hold
 - Forward Busy/No Answer
 - Paging
 - Bridge Port (Local and Remote only)

- 8 If applicable, enter the digits that prevent a certain type of call from proceeding in the Disabled Outbound Digit Sequence box.
- 9 Specify the positions of the Local Call Keys.

Note: Key 0 is not recommended for ports defined as local and remote. Keys 8 and 9 are recommended. You can select Key 0 if the port is configured as local only.
- 10 Click OK to save the information in the temporary work file.
- 11 To update the Remote Office 9150 unit with the new information, click Send.

IF you are	THEN
logged on to the Remote Office 9150 unit	the changes are written into the Remote Office 9150 unit's buffer. To save the changes in flash memory, choose Upload/Download → Save to Flash.
not logged on to the Remote Office 9150 unit	The Connection not Established dialog box appears. Do one of the following: ■ Log on to the Remote Office 9150 unit, and then click Send again. ■ Save the changes to a file on your administration PC.

Configuring DSP resources

This section shows you how to configure DSP resources on your Remote Office 9150 unit. The Remote Office 9150 unit must provide the same number of voice DSP channels as the maximum number of simultaneous calls your remote services network supports. Each DSP *module* holds two DSP *devices*. Currently, each DSP *device* holds four DSP *channels*. To add eight DSP *channels* to your Remote Office system's voice processing capability, add one DSP application *module*.

Getting there 9150 → Configuration Manager → DSP Configuration

DSP Configuration property sheet

DSP CONFIGURATION

Module Number: 0

No of Devices: 2

Device Number 1

DSP Load: AUTO

Compression Algorithms: G729, G726, G711

Device Number 2

DSP Load: AUTO

Compression Algorithms: G729, G726, G711

OK Default Send Retrieve Help

Module identification

The upper portion of the DSP configuration property sheet displays fields that identify the module you are currently configuring. In the Module Number drop down box, choose the module position on the Remote Office 9150 unit that the DSP module occupies. Module 0 represents the built-in DSP resources on the Remote Office 9150 unit—the equivalent of one DSP application module.

Device configuration

The middle portion of the property sheet displays information describing the DSP loads, and corresponding compression algorithms that you can select for each DSP device.

Configuring DSPs

To configure DSP modules on your Remote Office 9150 unit, complete the following steps:

- 1 Access the DSP Configuration property sheet.
- 2 Complete the fields as described in “DSP Configuration field descriptions” on page 237.
- 3 Click on the **OK** button to save the information in the temporary work file.
- 4 Click on the **Send** button to update the Remote Office 9150 unit with the new information.

Result: The Remote Office 9150 unit writes changes to a temporary file on the administration PC.

Note: To save changes to the Remote Office 9150 unit's flash memory, select Upload → Save to Flash.

DSP Configuration field descriptions

Field	Description
Module Number	Select the number of the module DSP position on the Remote Office 9150 unit occupied by the DSP application module you are configuring. Valid options are: 1–4.
No of Devices	This is a read-only field displaying the number of DSP devices on the application module in the selected module position. Refer to “Configuring DSPs” on page 236 for an explanation of DSP <i>devices</i> versus DSP <i>modules</i> and DSP <i>channels</i> .
DSP Load	Select the DSP load that you want to enable on this DSP device. Valid options are: G729, AUTO.
Note: This description applies to both appearances of this field.	Note: Nortel Network’s recommends that you select AUTO .
Compression Algorithms	This read-only field displays the compression algorithms contained in DSP load displayed in the DSP load drop down box.
Note: This description applies to both appearances of this field.	

Chapter 6

Using Remote Office 9150 stations

In this chapter

Modes of operation	240
Placing and receiving calls	244
Indicator updates	248
Display messages	250
Telephone features operation	253
Going online and offline	257

Modes of operation

Digital telephones at your Remote Office 9150 site can operate in the following modes:

- host-controlled
- locally controlled
- online to host PBX
- offline from host PBX

Host-controlled mode

Host-controlled mode means that the host PBX controls the following:

- some display messages that appear on your telephone
- indicator updates such as the message waiting indicator
- calls that you receive from or place to someone at the host PBX site

In host-controlled mode, a voice path is established to the host PBX and signaling messages are passed between the host PBX and the Remote Office 9150 unit.

Exception: If Local Switchover is enabled, and the station-to-station call is completed through the host PBX, signaling messages are passed between the host PBX and Remote Office 9150 unit normally. However, the voice path is established by the Remote Office 9150 unit without consuming host connection bandwidth. The host PBX is aware that the call is active and tracks the status of the phoneset.

If the call cannot be completed through the host PBX, you hear a reorder dial tone.

Locally Controlled mode

Local-controlled mode means that the Remote Office 9150 unit at your site controls the following:

- calls to other stations at this site
- calls that are made to or received from your community through your local telephone service provider

Relationship between host-controlled and locally controlled modes

Both the host-controlled and locally controlled modes can be used at the same time. When placing or receiving calls, the call modes are controlled by the following telephone keys:

- the host call appearance key (also known as the *primary DN* key)
- the local call appearance key (can sometimes be referred to as the *secondary DN* key)

Host call appearance key

The host call appearance key is the main key you use to place and receive calls. For example, if someone from Finance at Head Office calls you, the call rings on this key. Similarly, if you need to call someone in Payroll at Head Office, you place the call on this key.

Local call appearance key

The local call appearance key is the key you use to place and receive local calls. For example, if your office is working overtime and everyone wants pizza, you call the pizza delivery place on the local call appearance key. Similarly, you use this key if you want to call one of your customers or suppliers or someone else at your site.

Your telephone can have up to two local call appearance keys. Your system administrator can tell you where these keys are and how they are labeled.

Online mode

When in online mode, calls initiated on the host call appearance key are directed through the host PBX. Any long distance charges associated with calls placed through the PBX over the PSTN are charged to the host PBX site. The display on all digital telephones shows "Online Mode."

Offline mode

When in offline mode, you cannot place calls through the host PBX over either the IP network or PSTN. You can only place calls through your local telephone service provider if your station has been granted locally controlled call capability. The display on all digital telephones show "Offline Mode."

Why offline mode is important

Your organization is concerned about telephone costs and, as such, wants to ensure that the ISDN BRI line at your site is used for host-controlled calls during business hours only. This is especially important when the ISDN BRI connection between the host PBX and your site is defined as *permanent* (always on) rather than *on demand*. A permanent ISDN BRI connection means the line remains active all the time and incurs charges unless it is put into offline mode.

What controls the online and offline modes

The online and offline modes can be controlled by one or both of the following:

- the online/offline schedule configured for your site on the RLC at the host PBX
- special prefix (SPRE) codes configured on the Remote Office 9150 unit at your site

Online/offline schedule at host PBX

If telephone service costs are an issue, your telecom network administrator defines an online/offline schedule on the RLC port to which your site is assigned. The times at which your site is put into online or offline mode are processed by the host PBX.

For example, if your normal business day is from 9:00 a.m. to 5:00 p.m. from Monday to Friday, the schedule for your site instructs the host PBX to put all stations at your site into online mode during those times. For all other time periods, all stations are in offline mode and, therefore, disconnected from the host PBX.

Note: If you initiate a call on a host call appearance key on any station, then full functionality is allowed even if the time period is outside the automatic offline periods defined on the RLC.

SPRE codes used at your site

If SPRE codes have been defined on the Remote Office 9150 unit at your site, your site can control the times at which stations are put into online or offline modes. You do this by entering one of the following codes on any digital telephone at your site:

- Online SPRE code
- Offline SPRE code

It is recommended that one person at your site be designated as the person responsible for putting the Remote Office 9150 unit (and all stations) into online mode at the beginning of the business day, and into offline mode at the end of the day.

For information about going online or offline, see page 257.

Placing and receiving calls

The way in which you place outgoing calls depends on the call appearance key you use to place the call.

The call appearance key on which calls are received depends on where the call is coming from.

Receiving incoming calls

The calling line identification (CLID) of an incoming call determines which call appearance key accepts the call.

IF the call	THEN the call
information contains a Called Party Number Display (CPND) that matches a telephone number assigned to one of the ISDN BRI B-channels from your telephone service provider	is routed to the station based on the DN's to Alert configuration on the trunk group to which the B-channel belongs. If the DN's to Alert fields are blank, the call rings on all stations. The call rings on the first local call appearance key on all stations that have been designated to receive calls from this trunk. Note: If the first call appearance key is already busy with a call, the call is presented on the second call appearance as a call waiting. The indicator flashes and an alert tone sounds.
comes in on the communication path between the RLC and Remote Office 9150 unit	is routed to the station based on the Remote Office 9150 station to RLC port assignment in the Remote Office 9150 unit's ports configuration. The call rings on the host call appearance key.
information contains the DN of another station at this site	rings on the local call appearance key.

Methods for placing outgoing calls

You can place an outbound call from a Remote Office 9150 station in one of the following ways.

- **Method 1: Pick up the handset.**

This method automatically initiates a host-controlled call.

Note: If you then press the local call appearance key, the dial tone from the host PBX is changed to locally controlled mode, and the host PBX connection is released.

- **Method 2: Press a call appearance key.**

When you press the host call appearance key, a host-controlled call is initiated. When you press the local call appearance key, a locally controlled call is initiated.

To place host-controlled calls

- 1 Pick up the handset or press the host call appearance key.

Result: A connection is established with the host PBX and you hear dial tone.

Note: If a connection to the host PBX cannot be established within a time-out period or no resources are available to carry the call, you hear a reorder dial tone (a fast busy signal), and the following message appears on the telephone display:

Release and Try Again

- 2 Dial the number of the party you want to call.

Result: The host PBX receives and processes the dialed digits and rings the called party.

To place outgoing locally controlled calls

Note: You cannot use this procedure to place calls to the host PBX site. If you try, you hear a reorder dial tone (a fast busy signal) and the following message appears on your telephone display:

Release and Try Again

- 1 Do one of the following:

IF you are using	THEN
an analog or ATA-equipped station	do the following: - a Pick up the handset. Result: A connection is established with the host PBX and you hear a dial tone. - b Dial the Local Calling SPRE code. Result: The connection is switched to the Remote Office 9150 unit and you hear a dial tone.
a digital telephone	pick up the handset, and then press a local call appearance key. Result: A connection is established with the Remote Office 9150 unit and you hear a dial tone.

- 2 Dial a trunk access code, if required.

Result: The Remote Office 9150 unit obtains a free trunk and you hear another dial tone.

Note: If a trunk is not available, you hear a reorder dial tone (a fast busy signal) and the following message appears on the telephone display:

Release and Try Again

- 3 Dial the number of the party you want to call.

Result: Your local telephone service provider receives and processes the dialed digits and rings the called party.

To call another station at your site

Station-to-station calls should be attempted through the host PBX to allow all stations configured as multiple appearance DN (MADNs) to ring and provide access to voice mail if the call is not answered.

If a connection cannot be established through the host PBX, then you can use the local call appearance key to place the station-to-station call.

- 1 Pick up the handset or press the host call appearance key.

Result: A connection is established with the Remote Office 9150 unit and you hear a dial tone. The indicator beside the host call appearance key lights.

- 2 Dial the extension of the party you want to call.

Result: The host PBX receives and processes the dialed digits, and rings the station as well as any other stations that include the dialed DN as an MADM appearance.

Note: The MADM stations could be located at another site (such as the host PBX site).

IF the call is
answered by

THEN

an MADM station
at another site

a voice path to the host PBX is established and the
call proceeds.

a station at
this site

all signaling continues to be processed by the host
PBX. However, the actual voice path is connected
between the two stations and the Remote Office
9150 unit. No trunk bandwidth back to the host PBX
is used for the voice path. Trunk bandwidth
previously reserved for the call is released and
made available to other calls.

Indicator updates

Digital telephone indicators reflect the current status of the telephone. For example, they identify when calls are waiting, active, or on hold, or, if your office has voice mail, that messages have been received.

Indicators are updated as follows:

- by the host PBX when a connection between the host PBX and Remote Office 9150 unit is active
- by the Remote Office 9150 unit for feature keys defined on stations with local call capability

Host-controlled indicator updates

Indicators for host-controlled features are updated automatically by the host PBX each time

- an incoming call is received by your site from the host PBX
- an outgoing call is made from your site through the host PBX
- a message waiting indicator (MWI) update is received by someone at your site

Note: If the PSTN is being used and the Remote Office 9150 unit is configured with a permanent (always on) connection to the host PBX, the ISDN BRI service is active and telephone indicators are always updated.

If the IP network is being used to route calls, indicators are always updated.

Locally controlled indicator updates

The following indicators are updated by the Remote Office 9150 unit (that is, these indicator updates are locally controlled):

- host and local call appearance key indicators
The indicator lights when the handset is taken off-hook, or when you press the call appearance key to go off-hook.

Note: The Remote Office 9150 unit passes key presses and the on- or off-hook status for the host call appearance key to the host PBX.

- Handsfree
- Mute

Display messages

This section describes the messages that can appear on your digital telephone display.

Message descriptions

Message	Description
Going Offline in 30 Secs	This message warns you that all digital telephones at this site are about to go offline in the number of seconds indicated. If any calls are active, they are disconnected when the offline mode is activated. To override, enter the Online SPRE code.
Going Offline in 20 Secs	
Going Offline in 10 Secs	
Hostless Mode	The connection to the host PBX cannot be established. The host PBX might be temporarily unavailable. You can still place local calls by using one of the local call appearance keys. Note: If Hostless Mode persists, contact your system administrator.
Logged In	If this message appears on your station, then your station is associated with a multi-user or dynamic pool port on the RLC, and it is in logged on status. Note: This message appears for approximately ten seconds.
Offline Mode	You cannot place calls through the host PBX over either the IP network or the PSTN. Note: If you need to place a call through the host PBX while in offline mode, press the host call appearance key. This establishes a connection to the host PBX and puts all digital telephones at your site into online mode.

Message	Description
Online Mode	You can place and receive calls through the host PBX.
Port Already in Use	If this message appears on your station, then your station is associated with a multi-user or dynamic pool port on the RLC. This message appears if the port to which you are attempting to log on is already being used by someone else.
Port Not Logged In	If this message appears on your station, then your station is associated with a multi-user or dynamic pool port on the RLC, but it is in logged off status.
QoS Recovery	The QoS has returned to normal on the IP network and your active call is being automatically moved to the IP network.
QoS Transition	The QoS has degraded on the IP network and your active call is being automatically moved to the PSTN.
Release and Try Again	All Remote Office 9150 trunks are busy or there are not enough DSP resources to process the call. Try again at a later time. Note: Ensure the call you are placing is initiated from the appropriate call appearance key: ■ host call appearance key: to call someone at the host PBX site ■ local call appearance key: to place a local PSTN call or to call another station at your site
Bandwidth Limit	If you see this message and hear a fast busy signal when you attempt to place a call, then there is insufficient PSTN bandwidth. Wait a moment, and then try your call again.

Message	Description
DSP Limit	If you see this message and hear a fast busy signal when you attempt to place a call, then Digital Signal Processor (DSP) resources are all busy. Wait a moment, and then try your call again.
Call Failure	If you see this message and hear a fast busy signal when you attempt to place a call, then the Remote Office 9150 unit failed to establish the PSTN connection to the RLC. Wait a moment, and then try your call again.

Telephone features operation

This section describes how to use the following digital telephone features in host- or locally controlled modes:

- emergency service calls
- Hold
- Call Waiting
- Call Transfer
- Conference
- Call Forward
- Paging

Note: The Conference and Call Forward features are supported for host-controlled calls only.

Emergency service calls

The Remote Office 9150 unit allows an emergency number (for example, 911 in North America) to be programmed by your system administrator.

If the PSTN is used to route calls, and someone dials this emergency service number on any station that is connected to the Remote Office 9150 unit, the call is processed by your local telephone service provider.

You can initiate the emergency service call on either the host call appearance (primary DN) key or local call appearance key. You do not have to dial a trunk access code first.

ATTENTION

If only the IP network is being used to route calls, you must use a telephone that is directly connected to the PSTN to place an emergency service call. If you place the call on a station that is connected to the Remote Office 9150 unit, the call is routed through the host PBX, which can in a different city.

Hold

How Hold works in host-controlled mode

When you press Hold on a host-controlled call, the holding party receives the Hold treatment defined on the host PBX. For example, if the host PBX is configured to play music to holding parties, then the holding party hears music.

You can press any available call appearance key to place a new call.

How Hold works in locally controlled mode

Normally, you put a call on hold by pressing Hold. However, you can also put a locally controlled call automatically on hold by pressing the other local call appearance key. To use this feature, Auto Hold must be enabled on your station.

If Auto Hold is not enabled, and you press a local call appearance key while a call is active on the other local call appearance key, that call is disconnected.

When you press Hold on a locally controlled call, the holding party hears silence. You can press any available call appearance key to place a new call.

Call Waiting

Since the Remote Office 9150 unit does not use host-controlled indicators and the locally controlled indicators are not defined on the host PBX, there are never any indicator conflicts when a call is presented to the station.

However, since the host PBX is not aware when locally controlled calls are active, the host PBX might try to present a call and ring your station while you are busy with a locally controlled call. The Remote Office 9150 unit always checks the status of your station before ringing it. If your station is busy with a call, the alert tone is sounded instead.

How Call Waiting works in host-controlled mode

If you are busy with a host-controlled call, incoming calls are handled as follows:

- An incoming host-controlled call is directed to the call waiting key by the host PBX.
- An incoming locally controlled call flashes the local call appearance key indicator and sounds the alert tone.

How Call Waiting works in locally controlled mode

If you are busy with a locally controlled call, incoming calls are handled as follows:

- An incoming host-controlled call flashes the host call appearance key and sounds the alert tone.
- An incoming locally controlled or station-to-station call flashes the next available local call appearance key and sounds the alert tone. If both local call appearance keys are busy, then the call is not presented to your station.

Call Transfer

Call transfer works the same way in both host- and locally controlled modes. The only difference is the treatment the holding party receives, depending on whether the original call is a host-controlled or locally controlled call.

A call on the host call appearance key can be transferred

- to another station that has remote call capability at this site
- to a station at the host PBX site

A call on the local call appearance key can only be transferred to another station at this site. You cannot transfer a call on the local call appearance key to a station at the host PBX site.

For both, you can do an announced or unannounced (blind) transfer.

To transfer a call

- 1 Press the Transfer key.

Result: The active call is placed on hold and you hear a dial tone.

- 2 Dial the number to which you want to transfer the call.
- 3 Press the Transfer key again to complete the transfer.

Note: You can press the Transfer key while the call is still ringing, or after the called party answers.

Conference

The Conference feature is supported for host-controlled calls only. You cannot conference in someone who must be called through the local PSTN.

To place a conference call

- 1 Press the Conference key.

Result: The active call is placed on hold and you hear a dial tone.

- 2 Dial the number of the party you want to conference in.
- 3 When the called party answers, press the Conference key again to complete the conference.

Call Forward

Call Forward is supported for host-controlled calls only. Your station might be programmed to forward all calls, forward calls when your station is busy, or forward calls when you do not answer.

Paging

When you press a local call appearance key, and then dial the Paging SPRE code, you can announce a page to all other stations at your site.

Note: You can disable Paging for any station.

Going online and offline

Stations at the Remote Office 9150 site operate in either online mode or offline mode. This is controlled by one or both of the following:

- SPRE codes to manually toggle all stations at your site between online and offline modes
- an online/offline schedule on the host PBX to automatically toggle all stations at your site between online and offline modes

For a description of the online and offline modes, see “Modes of operation” on page 240.

To use the SPRE code to put all stations into online mode

- 1 Lift the digital telephone handset, or press one of the local call appearance keys.
- 2 Dial the pound key (# in North America) followed by the Online SPRE code.

Note: To learn this code, consult with your system administrator.

Result: The connection to the host PBX is initiated and negotiated with the host PBX. During this negotiation period (up to 5 seconds), stations at your site cannot be used for host-controlled calls. When negotiation is completed and connection to the host PBX has been established, Online Mode appears on the telephone display.

To use the SPRE code to put all stations into offline mode

- 1 Lift the digital telephone handset, or press one of the local call appearance keys.
- 2 Dial the pound key (# in North America) followed by the Offline SPRE code.

Note: To learn this code, consult with your system administrator.

Result: Offline Mode appears on the telephone display.

To override an automatic offline event from the host PBX

If the host PBX attempts to process an offline event while you are on a host-controlled call, you are alerted by both an audible alert and a display message indicating that you are about to go offline in 30, 20, or 10 seconds. If you ignore this warning, your call will be disconnected.

To prevent your call from being disconnected, enter the online SPRE code. You can do this without putting your call on hold first. The online SPRE code cancels the offline event, leaving all stations online until the next offline event occurs.

Chapter 7

Administration

In this chapter

Changing the administration password	260
Section A: Performing backups and restores	265
Section B: Working with system logs	273
Section C: Viewing statistics	279
Section D: Performing upgrades	309

Changing the administration password

The Remote Office 9150 unit's configuration is protected by two layers of password security. If you want to secure the Remote Office 9150 unit's configuration so that others cannot make configuration changes, you should change the following:

- the Configuration Manager password
This password prevents unauthorized offline configuration changes from being performed.
- the Remote Office 9150 unit's password
This password prevents unauthorized online changes of the configuration residing in the Remote Office 9150 unit's flash memory.

ATTENTION

Ensure that you record the passwords and store them in a safe, secure place. If you forget or lose the password, you must contact your Nortel Networks technical support representative.

Getting there 9150 → Configuration Manager

To change the Configuration Manager password

- 1 From the menu, choose Connect → Change Password → Local.
Result: The Change Password - Local dialog box appears.

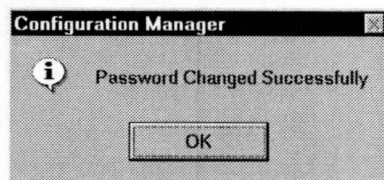


- 2 Complete the fields as described in "Password dialog box field descriptions" on page 263.
- 3 Click OK.

IF the password change THEN

was successful

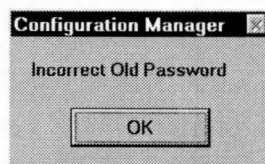
the following appears:



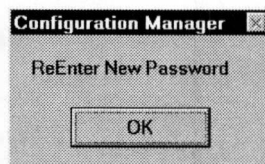
Click OK.

was not successful

one of the following messages appears:



was not successful
(continued)

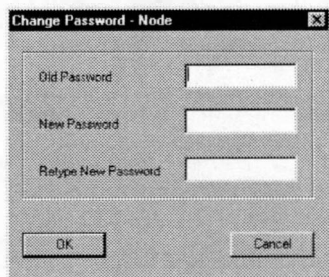


Click OK, and then try again.

To change the Remote Office 9150 unit's password

- 1 From the menu, choose Connect → Change Password → Node.

Result: The Change Password - Node dialog box appears.

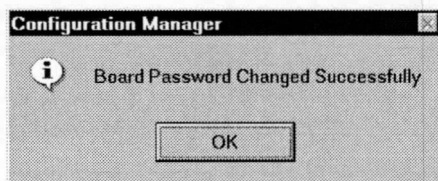


- 2 Complete the fields as described in "Password dialog box field descriptions" on page 263.
- 3 Click OK.

IF the password change THEN

was successful

the following appears:



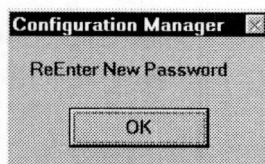
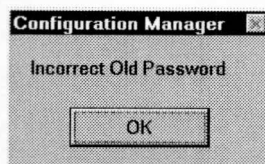
Note: This means the password has been written to the Remote Office 9150 unit's flash memory.

Click OK.

IF the password change THEN

was not successful

one of the following messages appears:



Click OK, and then try again.

- 4 From the menu, choose Upload/Download → Save to Flash.
Result: The Remote Office 9150 unit's flash memory is updated with the new password.
- 5 Restart the Remote Office 9150 unit.

Password dialog box field descriptions

Field	Description
Old Password	Enter the existing password.
New Password	Enter the new password.
Retype New Password	Enter the new password again.

Section A: Performing backups and restores

In this section

Creating a backup configuration file	266
Restoring the configuration	268

Creating a backup configuration file

Create a backup copy of the Remote Office 9150 unit's configuration by downloading the Remote Office 9150 unit's configuration from flash memory to a text file on your administration PC.

When to create a backup

Nortel Networks recommends that you create a backup of your configuration file whenever you make configuration changes or after you perform a firmware upgrade.

Storing backup configuration files

The Remote Office 9150 unit is an extension of the telecommunications and data network. It is extremely important that you keep a backup copy of the Remote Office 9150 unit's configuration. If the Remote Office 9150 unit's flash memory or configuration becomes corrupted or is lost, you can easily restore it.

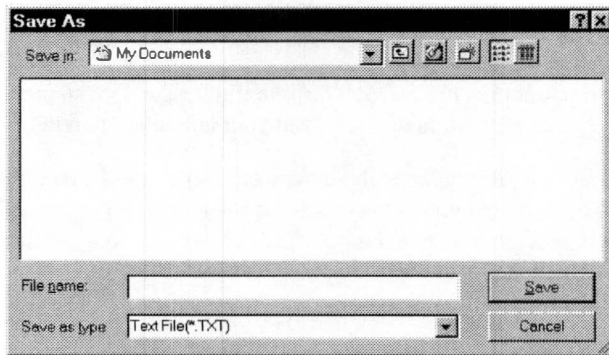
Store the configuration file in a safe, secure location, such as on backup tape or other media that is stored offsite.

Nortel Networks recommends that you keep the backup files indefinitely.

Getting there 9150 → Configuration Manager

To create the backup file

- 1 From the menu, choose Upload/Download → Download Configuration.
Result: The Save As dialog box appears.



- 2 Navigate to the folder where you want to put the configuration text file.
- 3 Enter a name for the file in the File name box.

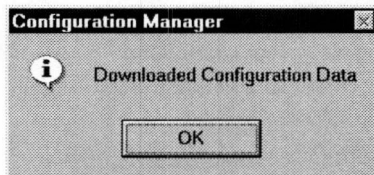
Note: This configuration file will become your backup file, so ensure the file name is meaningful. The file name's extension is .TXT.

- 4 Click Save.

Result: The Save As box closes, and the following message appears in the status bar at the bottom of the screen:

Downloading Config From Board

When completed, the following appears:



- 5 Click OK.

Restoring the configuration

Restore the Remote Office 9150 unit's configuration in flash memory by uploading a configuration text file from your administration PC.

The upload is performed over the IP network using the TFTP protocol. You must have a TFTP server application running on your administration PC. The TFTP server's base directory must point to the directory that contains the configuration file you want to upload.

Before you begin

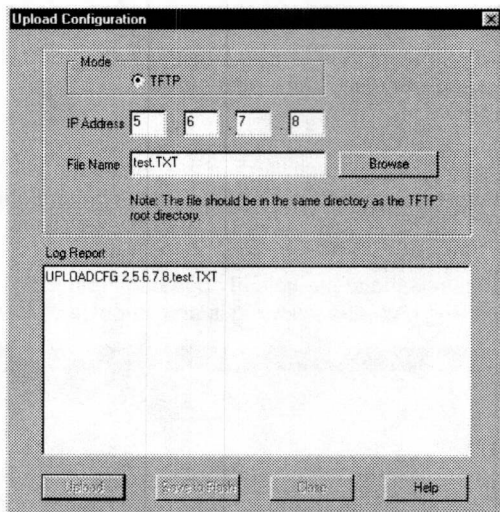
Before you can upload the configuration file to the Remote Office 9150 unit, you must do the following:

- 1 Start the TFTP server application.
- 2 Ensure the TFTP base directory reflects the directory where the configuration file you want to upload is located.

Getting there 9150 → Configuration Manager

To upload a configuration file over the IP network

- 1 From the menu, choose → Upload/Download → Upload Configuration.
Result: The Upload Configuration screen appears.

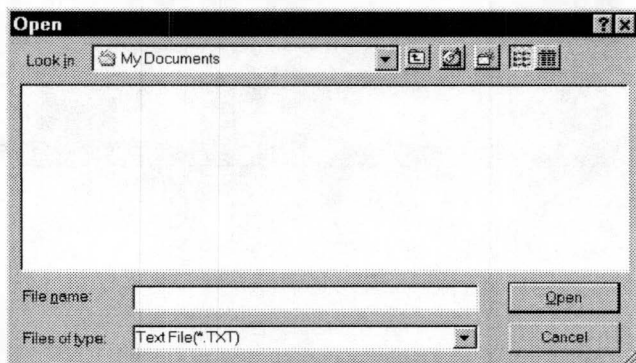


- 2 In the IP Address boxes, enter the IP address of the TFTP server.

Note: Since the TFTP server application is running on your administration PC, this is the IP address of the PC.

- 3 Click Browse.

Result: The Open dialog box appears.



- 4 Ensure the Files of type box shows Text File(*.TXT).

- 5 Navigate to the folder in which the configuration file is located.
- 6 Select the file, and then click Open.

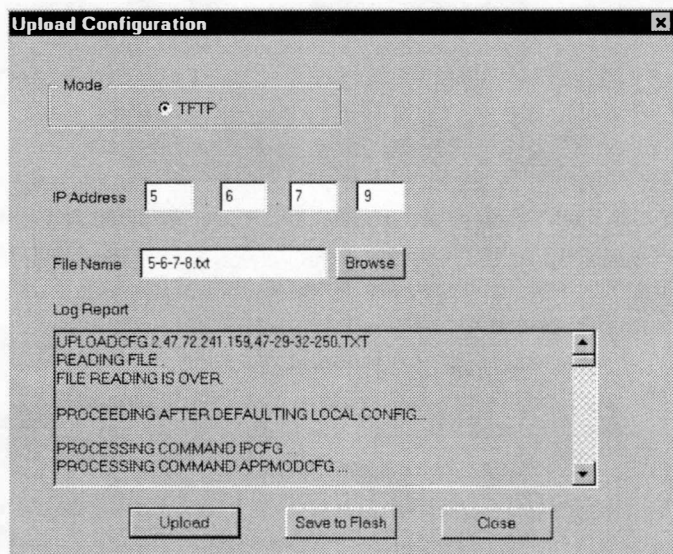
Result: You are returned to the Upload Configuration dialog box. The file you selected is shown in the File Name box.

- 7 Click Upload.

Result: If the file opens successfully, then the upload proceeds. The following message appears in the status bar at the bottom of the screen:

Uploading Config to Board

Status messages relating to the upload appear in the middle of the Upload Configuration dialog box. The following is an example.



**CAUTION**

Risk of incorrect operation due to partial configuration

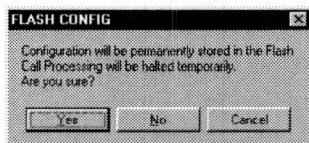
Do not interrupt the configuration upload. If you interrupt the configuration upload, this results in an incomplete configuration in the Remote Office 9150 unit's database.

If the configuration upload is interrupted, repeat this procedure immediately.

IF the upload was	THEN
successful	The following message appears: CONFIG UPLOAD SUCCESSFUL... USE SAVECFG TO UPDATE FLASH. Go to step 8.
not successful	the following message appears in the middle of the Upload Configuration dialog box: CONFIG UPLOAD FAILED For further instructions, see Chapter 8, "Troubleshooting."

- 8 On the Upload Configuration screen, click Save to Flash.

Result: The following dialog box appears:



- 9 Click Yes.

Result: The following message appears in the status bar at the bottom of the screen:

Saving to Flash in Progress

When the save is finished, the following message appears in the middle of the Upload Configuration dialog box:

CONFIGURATION IS UPDATED INTO FLASH...

- 10 Click Close.

- 11 Restart the Remote Office 9150 unit.

Note: For instructions, see "Performing a system restart or shutdown" on page 177.

Section B: Working with system logs

In this section

Displaying logs	274
Resizing logs	276
Clearing logs	277

Displaying logs

The Remote Office 9150 unit keeps track of system performance through the maintenance of logs. Each line stored in the log represents a separate action completed by the unit.

Use these logs when you want to troubleshoot system problems. You can print the log to a text file by copying the information from the log window, and then pasting it into a text file.

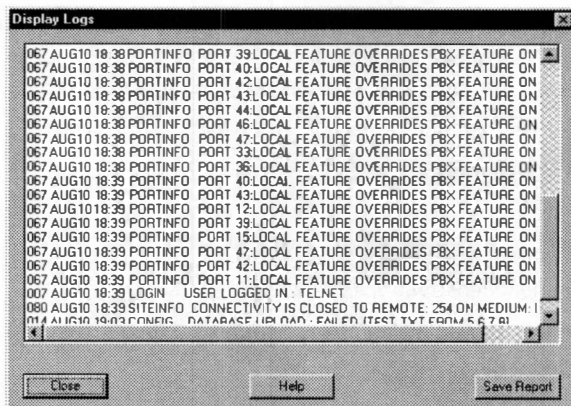
For a description of the Display log messages refer to Appendix D, “Display log definitions,”.

Getting there 9150 → Configuration Manager

To display logs

From the menu, choose Alarms/Stats/Logs → Display Logs.

Result: The Remote Office 9150 unit displays the logs it maintains in a window similar to the following. You can use the scroll bar to browse through the logs to find the information in which you are interested.



Note: The information displayed in these logs also appears in the event.dat file on your administration PC.

To print the log to a file

If you are requesting technical support, you might be asked to provide a copy of the logs. To recreate the log in a file on your administration PC, follow this procedure:

- 1 Position the mouse pointer inside the log window at the beginning of the text you want to copy.
- 2 Select the text you want to copy, and then press Ctrl-C.
- 3 Open WordPad or Notepad.
- 4 Press Ctrl-V to paste the text.
- 5 Save and close the text file.

Resizing logs

The log maintains a maximum of 1000 lines of text. When the log reaches 1000 text lines, new text lines overwrite existing lines.

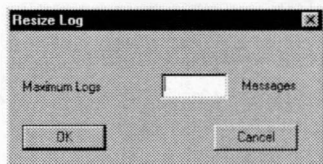
You might find that you want the logs to occupy a larger or smaller percentage of memory on the Remote Office 9150 unit. You can use the following procedure to change the size of the logs that the Remote Office 9150 unit keeps.

Getting there 9150 → Configuration Manager

To change the size of Remote Office 9150 unit logs

- 1 From the menu, choose Alarms/Stats/Logs → Resize Logs.

Result: The Resize Log dialog box appears.



Note: The queue size, in this case, means the number of text lines in the log. The log currently holds a maximum of 1000 text lines.

- 2 Enter the maximum number of text lines you want to maintain in the log.
- 3 Click OK.

Clearing logs

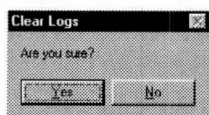
The Remote Office 9150 unit allows you to increase memory by clearing the log queue. Use the following procedure to discard information from the logs that is no longer useful.

Getting there 9150 → Configuration Manager

To clear logs

- 1 From the menu, choose Alarms/Stats/Logs → Clear Logs.

Result: The CLEAR LOGS dialog box appears.



IF you select

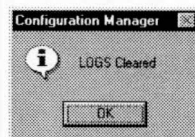
THEN

No or Cancel

the dialog box closes and the logs remain as is.

Yes

the Remote Office 9150 logs are cleared and the following confirmation dialog box appears:



Click OK.

Section C: Viewing statistics

In this section

Trunk Connection Statistics screen	280
Bandwidth Connection Statistics screen	282
Caller Information Statistics screen	284
Hardware Statistics screen	287
DSP screen	289
Ethernet Interface Statistics screen	292
BRI Statistics screen	295
Local Call Statistics screen	297
Remote Call Statistics screen	299
Device Information screen	301
ISDN Module Information screen	303
Network Statistics screen	305

Trunk Connection Statistics screen

The Trunk Connection Statistics screen allows you to see the amount of traffic that is processed over each B-channel. Use this statistics log to determine which trunks get used the most.

Getting there 9150 → Configuration Manager

To display the trunk connection statistics

- 1 From the menu, choose Alarms/Stats/Logs → Trunk Connection Statistics.
Result: The Trunk Connection Statistics screen appears.

Wait while Configuration Manager gathers statistics from the Remote Office 9150 unit's system logs.

Result: The statistics appear. The following is an example.

[illegible]

- 3 Do one of the following:
 - To refresh the statistics, click Refresh.
 - To close the statistics screen, click Close.

Trunk Connection Statistics field descriptions

Column	Description
Trunk Number	9150 - Identifies the ISDN BRI module and B-channel used for the call.
Status	Identifies the current status of the trunk. Valid options are: Active and Idle.
Call Type	Identifies whether the call is a local call or a remote signaling call. Valid options are: Local and Signaling.
Remote ID	Identifies the remote unit involved in the call.
Called Number	Identifies the remote DN regardless of who initiated the call.
Start Time	Identifies the time that the call began.
Duration	Identifies the amount of time taken for the call.

Bandwidth Connection Statistics screen

The Bandwidth Connection Statistics screen allows you to see how much bandwidth the Remote Office 9150 unit can use, and how much is actually being used. Use this statistics log to help you determine if you need to add more bandwidth on PSTN or IP connections.

Getting there 9150 → Configuration Manager

To display the bandwidth connection statistics

- 1 From the menu, choose Alarms/Stats/Logs → BW Connection Statistics.
Result: The Bandwidth Connection Statistics screen appears.
- 2 Wait while Configuration Manager gathers statistics from the Remote Office 9150 unit's system logs.

Result: The statistics appear. The following is an example.

[illegible]

- 3 Do one of the following:
- To refresh the statistics, click Refresh.
 - To close the statistics screen, click Close.

Bandwidth Connection Statistics field descriptions

Column	Description
Remote Unit Number	Identifies the remote unit that initiated the call.
Signaling Status	Identifies whether a connection is up on this unit. Valid options are: Active and Idle.
No of Voice Calls on IP	Identifies the number of calls in progress on this unit's IP connection.
No of Voice Calls on PSTN	Identifies the number of calls in progress on this unit's PSTN connection.
Used IP BW	Identifies the IP bandwidth in use on this unit.
Used Trunk BW	Identifies the PSTN bandwidth in use on this unit.
Total Up Trunk BW	Identifies the total PSTN bandwidth up and available to this unit.
IP QoS Status	Identifies the quality of service level on this unit's IP connection. Valid options are: Good and Bad.

Caller Information Statistics screen

The Caller Information Statistics screen allows you to see the types of calls being made (IP or PSTN), and how often QoS transitions occur. Use this statistics log to help you determine if the voice Quality of Service on your IP network is stable.

Getting there 9150 → Configuration Manager

To display the caller information statistics

- 1 From the menu, choose Alarms/Stats/Logs → Caller Info Statistics.

Result: The Caller Info Statistics screen appears.

- 2 Wait while Configuration Manager gathers statistics from the Remote Office 9150 unit's system logs.

Result: The statistics appear. The following is an example.

[illegible]

- 3 Do one of the following:
 - To refresh the statistics, click Refresh.
 - To close the statistics screen, click Close.

Caller Info Statistics field descriptions

Column	Description
Call Number	Identifies the number of the call that was processed by the Remote Office 9150 unit.
Remote ID	Identifies the board ID of the remote site that was involved in the call.
Connection ID	Identifies the serial number of this call through the lifetime of the logged on unit.
Remote ID	Identifies the unit ID of the involved remote unit.
Current Media	Identifies whether the call took place over the PSTN or IP network.
Type	Identifies the type of call. Valid options are: Signaling, Voice, and Local.
Priority	Identifies the priority setting of the involved trunk. Valid options are: PSTN Only, IP Only, High, and Normal.
Call BW	Identifies the amount of bandwidth used by the call.
Start Time	Identifies the time that the connection initiated.
Transitions to PSTN	Identifies the number of times the RLC moved the call to the PSTN.
Transitions to IP	Identifies the number of times the RLC moved the call to the IP network.

Column	Description
Last Transition to PSTN	Identifies the last time the RLC moved the call from the IP network to the PSTN.
Last Transition to IP	Identifies the last time the RLC moved the call from the PSTN to the IP network.

Hardware Statistics screen

The Hardware Statistics screen provides a listing of what modules you have installed in your Remote Office 9150 unit. Use it to determine which module positions in the Remote Office 9150 unit are populated, and what they contain.

Getting there 9150 → Configuration Manager

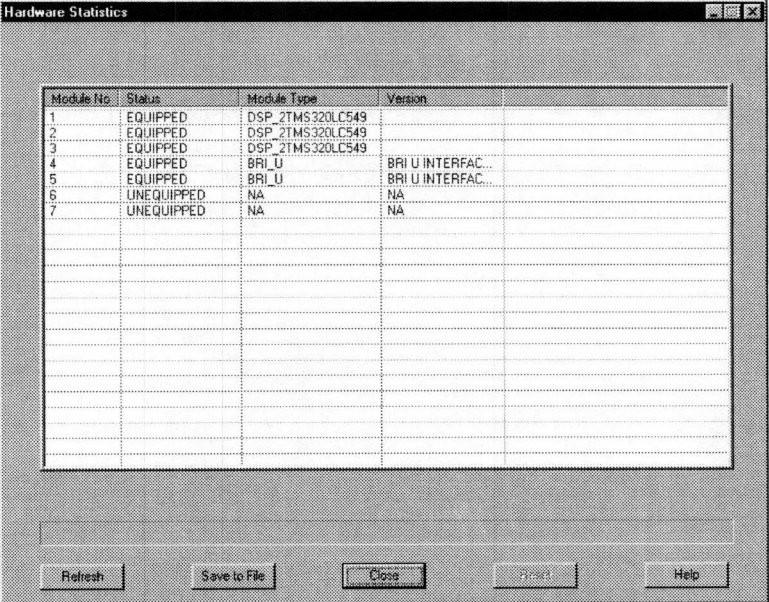
To display the hardware statistics

- 1 From the menu, choose Alarms/Stats/Logs → Hardware Statistics.

Result: The Hardware Statistics screen appears.

- 2 Wait while Configuration Manager gathers statistics from the Remote Office 9150 unit's system logs.

Result: The statistics appear. The following is an example.



The screenshot shows a window titled "Hardware Statistics" with a table of module information. The table has four columns: Module No., Status, Module Type, and Version. The data is as follows:

Module No.	Status	Module Type	Version
1	EQUIPPED	DSP_2TMS320LC549	
2	EQUIPPED	DSP_2TMS320LC549	
3	EQUIPPED	DSP_2TMS320LC549	
4	EQUIPPED	BRI_U	BRI_U INTERFAC...
5	EQUIPPED	BRI_U	BRI_U INTERFAC...
6	UNEQUIPPED	NA	NA
7	UNEQUIPPED	NA	NA

Below the table, there are five buttons: Refresh, Save to File, Close, Print, and Help.

- 3 Do one of the following:
 - To refresh the statistics, click Refresh.
 - To close the statistics screen, click Close.

Hardware Statistics field descriptions

Column	Description
Module No	Identifies the DSP application module's position on the Remote Office 9150 motherboard.
Status	Identifies whether there is a functional DSP application module in the position identified in the Module No field. Valid options are: Equipped, meaning that a DSP application module is installed in the module position, and Unequipped, meaning that there is not a DSP application module installed in the module position.
Module Type	Identifies the part number of the hardware installed in the module position.
Version	Identifies the version of DSP application module installed in the module position.

DSP screen

Digital Signal Processor (DSP) Statistics provide information about the DSP application modules installed on the logged-on RLC. Use this screen to determine the module positions that are populated, what type of DSP those positions contain, and the functionality provided by each module.

Getting there 9150 → Configuration Manager

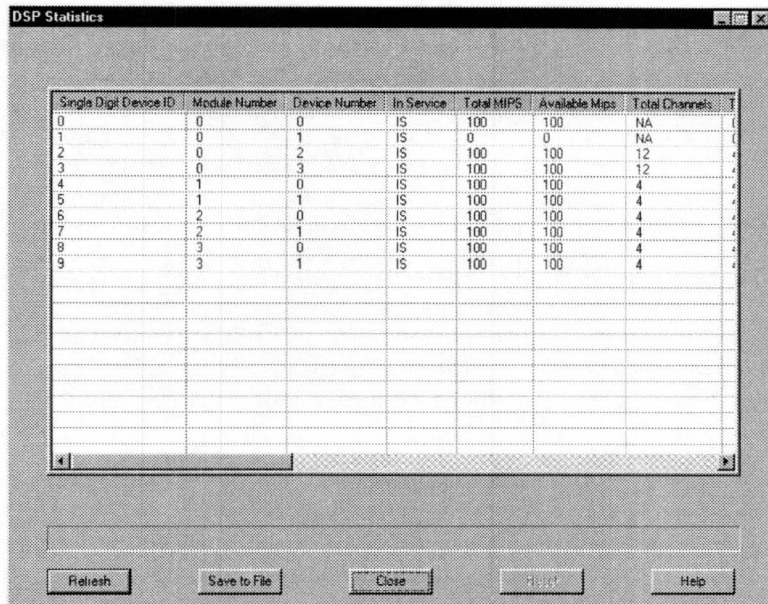
To display DSP statistics

- 1 From the menu, choose Alarms/Stats/Logs → DSP.

Result: The DSP screen appears.

- 2 Wait while Configuration Manager gathers statistics from the Remote Office 9150 unit's system logs.

Result: The statistics appear. The following is an example.



The screenshot shows a window titled "DSP Statistics" with a table of data. The table has 8 columns: Single Digit Device ID, Module Number, Device Number, In Service, Total MIPG, Available Mips, Total Channels, and a partially visible 8th column. The data is as follows:

Single Digit Device ID	Module Number	Device Number	In Service	Total MIPG	Available Mips	Total Channels	
0	0	0	IS	100	100	NA	
1	0	1	IS	0	0	NA	
2	0	2	IS	100	100	12	
3	0	3	IS	100	100	12	
4	1	0	IS	100	100	4	
5	1	1	IS	100	100	4	
6	2	0	IS	100	100	4	
7	2	1	IS	100	100	4	
8	3	0	IS	100	100	4	
9	3	1	IS	100	100	4	

Below the table are five buttons: Refresh, Save to File, Close, Help, and Help.

- 3 Do one of the following:
 - To refresh the statistics, click Refresh.
 - To close the statistics screen, click Close.

DSP Statistics field descriptions

Column	Description
Single Digit Device ID	Identifies an internal sequence number for indexing this DSP device among all others on the RLC.
Module Number	Identifies this DSP Application Module's module number on the RLC. Valid options are: 0, 1, 2, 3, 4.
Device Number	Identifies the DSP device that processed the call.
In Service	Identifies any voice channels operating on this DSP application module.
Total MIPS	Identifies the total millions of instructions per second (MIPS) capacity for this DSP device.
Available Mips	Identifies the millions of instructions per second (MIPS) currently available on this DSP device.
Total Channels	Identifies the total channel capacity for this DSP device.
Total Voice Channels	Identifies the total voice channel capacity for this DSP device.
Available Voice Channels	Identifies the number of unused voice channels on this DSP device.
Total Modem Channels	Identifies the number of channels on this DSP device that can transmit modem calls.
Available Modem Channels	Identifies the number of unused channels on this DSP that can transmit modem calls.

Column	Description
Total Flex Channels	Identifies the number of channels on this DSP that can provide multiple functionalities.
Available Flex Channels	Identifies the number of channels on this DSP currently available to provide multiple functionalities.
Total Tones Channels	Identifies the number of channels on this DSP that can transmit tones.
Total Reserved Channels	Identifies the number of special purpose channels on this DSP reserved for internal use.
Name	Identifies the name of the DSP load, that is, the combination of DSP algorithms, on the DSP module.

Ethernet Interface Statistics screen

Ethernet Interface Statistics provide information about the connection between the IP network and the logged-on RLC that is achieved over the RLC's Ethernet interface.

Getting there 9150 → Configuration Manager

To display the Ethernet Interface statistics

- 1 From the menu, choose **Alarms/Stats/Logs** → **Ethernet Interface Statistics**.

Result: The Ethernet Interface Statistics screen appears

- 2 Wait while Configuration Manager gathers statistics from the Remote Office 9150 unit's system logs.

Result: The statistics appear. The following is an example.

[illegible]

- 3 Do one of the following:
- To refresh the statistics, click Refresh.
 - To close the statistics screen, click Close.

Ethernet Interface Statistics field descriptions

Column	Description
Channel	Identifies the Ethernet device that the statistics on that line apply to. Valid options are: 1, 2.
LAN Drv	Identifies the LAN driver used by the call.
Admin	Identifies the desired state of the port.
Oper	Identifies the actual state of the port.
IfcType	Identifies the interface type used by the call.
IfcNo	Identifies the Ethernet interface used by the call. Valid options are: 0 (ELAN), 1 (CLAN).
MTUlen	Identifies the Maximum Transmission Unit for this interface.
Speed	Identifies the data rate of this interface.
In - Octet	Identifies the number of inbound bytes.
UPkts	Identifies the number of inbound packets sent only to this recipient.
MPkts	Identifies the number of inbound packets sent to multiple recipients.
Disc	Identifies the number of packets discarded by the interface.
Err	Identifies the number of error packets received by the interface.

Column	Description
Out - Octet	Identifies the number of outbound bytes.
UPkts	Identifies the number of outbound packets sent only to this recipient.
MPkts	Identifies the number of outbound packets sent to multiple recipients.
Disc	Identifies the number of outbound packets discarded by the interface due to resource problems.
Err	Identifies the number of outbound packets discarded due to errors.
QLen	Identifies the number of bytes in the interface's outbound queue.

BRI Statistics screen

The BRI Statistics screen allows you to see the operational BRI channels and the cross connections between those channels and telephone sets.

Getting there 9150 → Configuration Manager

To display the BRI statistics

- 1 From the menu, choose Alarms/Stats/Logs → BRI Statistics.

Result: The BRI Statistics screen appears.

- 2 Wait while Configuration Manager gathers statistics from the Remote Office 9150 unit's system logs.

Result: The statistics appear. The following is an example.

[illegible]

- 3 Do one of the following:
 - To refresh the statistics, click Refresh.
 - To close the statistics screen, click Close.

BRI Statistics field descriptions

Column	Description
Module Index	Identifies the port on which the call was made. Valid options are: 0-63.
Module Number	Identifies the module position of the ISDN BRI module. 9150 valid options are: 4, 5, 6 and 7.
Device Number	Identifies internal sequence number for indexing ISDN BRI devices.
In Service	Indicates successful initialization of the ISDN BRI module.
Usage	Bit-encoded field identifying the module as an ISDN BRI module.
Total Channels	Identifies the ISDN BRI module's working and non-working channels.
Available Channels	Identifies the working channels on the ISDN BRI module.
Cross Connect Type	Identifies the cross-connect type used by the ISDN BRI module. Valid options are: DS30X, AMB, REG and VHD.

Local Call Statistics screen

The Local Call Statistics screen allows you to see how many local calls were processed by the Remote Office 9150 unit, and how long they lasted. Use this statistics log to determine how much traffic is being processed through the local PSTN.

Getting there 9150 → Configuration Manager

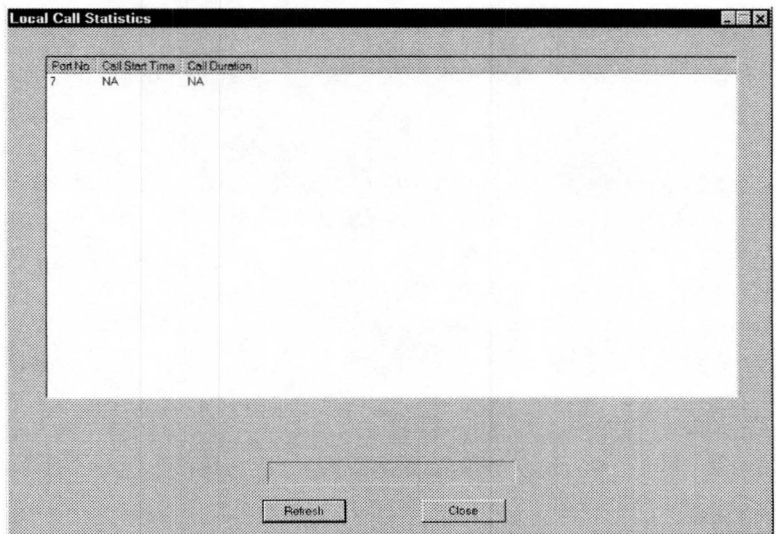
To display the local call statistics

- 1 From the menu, choose Alarms/Stats/Logs → Local Call Stats.

Result: The Local Call Statistics screen appears.

- 2 Wait while Configuration Manager gathers statistics from the Remote Office 9150 unit's system logs.

Result: The statistics appear. The following is an example.



- 3 Do one of the following:

- To refresh the statistics, click Refresh.
- To close the statistics screen, click Close.

Local Call Statistics field descriptions

Column	Description
Port No.	Identifies the Remote Office 9150 port through which the call was processed.
Call Start Time	Identifies the time when the call started.
Call Duration	Identifies the length of the call.

Remote Call Statistics screen

The Remote Call Statistics screen allows you to see how many calls were processed by the Remote Office 9150 unit through the host PBX, and how long they lasted. Use this statistics log to determine how much traffic is being processed through the host PBX.

Getting there 9150 → Configuration Manager

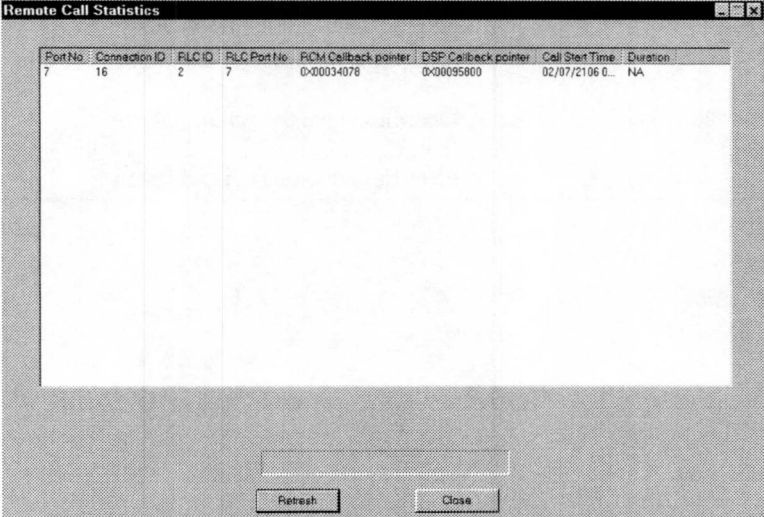
To display the remote call statistics

- 1 From the menu, choose Alarms/Stats/Logs → Remote Call Stats.

Result: The Remote Call Statistics screen appears.

- 2 Wait while Configuration Manager gathers statistics from the Remote Office 9150 unit's system logs.

Result: The statistics appear. The following is an example.



The screenshot shows a window titled "Remote Call Statistics". Inside the window is a table with the following columns: Port No., Connection ID, FLC ID, RLC Port No., PCM Callback pointer, DSP Callback pointer, Call Start Time, and Duration. The first row of data contains the values: 7, 16, 2, 7, 0x00034078, 0x00095800, 02/07/2106 0..., and NA. Below the table, there is a text input field and two buttons labeled "Refresh" and "Close".

Port No.	Connection ID	FLC ID	RLC Port No.	PCM Callback pointer	DSP Callback pointer	Call Start Time	Duration
7	16	2	7	0x00034078	0x00095800	02/07/2106 0...	NA

- 3 Do one of the following:

- To refresh the statistics, click Refresh.
- To close the statistics screen, click Close.

Remote Call Statistics field descriptions

Column	Description
ROU (Remote Office Unit) Port No.	Identifies the Remote Office 9150 port through which the call was processed.
Connection ID	A sequential number used for tracking individual calls.
RLC ID	Identifies the board ID of the RLC that processed the call.
RLC Port No	Identifies the RLC port that processed the call.
RCM Callback pointer	Identifies the internal program routine used. Note: This information is for technical support use only.
DSP Callback pointer	Identifies the internal program routine used. Note: This information is for technical support use only.
Call Start Time	Identifies when the call began.
Duration	Identifies how long the call lasted.

Device Information screen

Device Information Statistics screens allows you to see all telephones on the Remote Office 9150 unit, their capability and current status.

Getting there 9150 → Configuration Manager

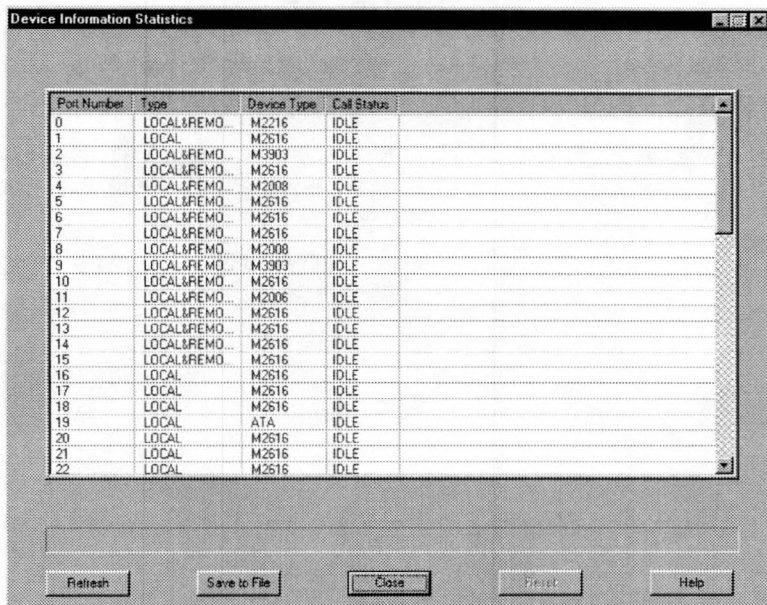
To display device information

- 1 From the menu, choose Alarms/Stats/Logs → Device Information.

Result: The Device Information screen appears.

- 2 Wait while Configuration Manager gathers statistics from the Remote Office 9150 unit's system logs.

Result: The statistics appear. The following is an example.



The screenshot shows a window titled "Device Information Statistics". Inside the window is a table with four columns: "Port Number", "Type", "Device Type", and "Call Status". The table lists 23 ports (0 to 22). Ports 0-9 are LOCAL&REMO, ports 10-15 are LOCAL&REMO, and ports 16-22 are LOCAL. Device types include M2216, M2616, M3903, M2008, and ATA. All call statuses are listed as "IDLE". At the bottom of the window are five buttons: "Refresh", "Save to File", "Close", "Print", and "Help".

Port Number	Type	Device Type	Call Status
0	LOCAL&REMO...	M2216	IDLE
1	LOCAL	M2616	IDLE
2	LOCAL&REMO...	M3903	IDLE
3	LOCAL&REMO...	M2616	IDLE
4	LOCAL&REMO...	M2008	IDLE
5	LOCAL&REMO...	M2616	IDLE
6	LOCAL&REMO...	M2616	IDLE
7	LOCAL&REMO...	M2616	IDLE
8	LOCAL&REMO...	M2008	IDLE
9	LOCAL&REMO...	M3903	IDLE
10	LOCAL&REMO...	M2616	IDLE
11	LOCAL&REMO...	M2006	IDLE
12	LOCAL&REMO...	M2616	IDLE
13	LOCAL&REMO...	M2616	IDLE
14	LOCAL&REMO...	M2616	IDLE
15	LOCAL&REMO...	M2616	IDLE
16	LOCAL	M2616	IDLE
17	LOCAL	M2616	IDLE
18	LOCAL	M2616	IDLE
19	LOCAL	ATA	IDLE
20	LOCAL	M2616	IDLE
21	LOCAL	M2616	IDLE
22	LOCAL	M2616	IDLE

- 3 Do one of the following:
- To refresh the statistics, click Refresh.
 - To close the statistics screen, click Close.

Device Information field descriptions

Column	Description
Port Number	Identifies the RLC port number to which the displayed information pertains.
Type	Identifies the port type. Valid options are: Remote, Data, or Local TCM.
Device Type	Identifies whether the telephone connection on the port identified above is Normal or ACD. Valid options are: Normal and ACD.
Call Status	Identifies whether the port is currently handling a call. Valid options are: Busy and Idle.
Login Status	Identifies whether the telephone connected to this port is active on the system. Valid options are: Logged on and Logged off. Note: This statistic applies only to ports to which ACD telephones connect.

ISDN Module Information screen

The ISDN Module Information statistics screen provides information about the ISDN BRI line. In particular you can use this statistics screen to determine if the BRI line is currently in use and the status of the link.

Getting there 9150 → Configuration Manager

To display ISDN module information

- 1 From the menu, choose Alarms/Stats/Logs → ISDN Module Information.

Result: The ISDN Module Information screen appears.

- 2 Wait while Configuration Manager gathers statistics from the Remote Office 9150 unit's system logs.

Result: The statistics appear. The following is an example.

[illegible]

- 3 Do one of the following:
- To refresh the statistics, click Refresh.
 - To close the statistics screen, click Close.

ISDN Module Information field descriptions

Column	Description
Module Number	Identifies the module position of the ISDN BRI module. 9150 valid options are: 4, 5, 6 and 7.
Module Type	Identifies the type of the ISDN BRI module. Valid options are: BRI-U, BRI-ST and INVALID.
Link Status	Identifies the current status of the ISDN BRI line. Valid options are: UP, DOWN, and INVALID.
Usage	Identifies whether the ISDN BRI line is in use or not. Valid options are: IDLE and ACTIVE.

Network Statistics screen

Network Statistics allow you to see the performance over the last 24 hours of the remote units connected to the logged-on RLC. Use these statistics to identify periods when other network activity can adversely affect Remote Office system performance. This screen shows remote unit performance in terms of the transmission and reception of frames and packets.

Getting there 9150 → Configuration Manager

To display network statistics

- 1 From the menu, choose Alarms/Stats/Logs → Network Statistics.

Result: The Network Statistics screen appears.

- 2 Wait while Configuration Manager gathers statistics from the Remote Office 9150 unit's system logs.

Result: The statistics appear. The following is an example.

Network Statistics

Remote Unit Number = 254 IP Address : 192.168.142.229

Hour	Tx Frames	Rx Frames	Rx Error	Rx Dropped	Error %	BroadCast Packet	Tx UCastPkt	Tx DiscPkt	
0	0	0	0	0	0.00	0	341	0	
1	0	0	0	0	0.00	3	1852	0	
2	0	0	0	0	0.00	0	0	0	
3	0	0	0	0	0.00	0	0	0	
4	0	0	0	0	0.00	0	0	0	
5	0	0	0	0	0.00	0	0	0	
6	0	0	0	0	0.00	0	0	0	
7	0	0	0	0	0.00	0	0	0	
8	0	0	0	0	0.00	0	0	0	
9	0	0	0	0	0.00	0	0	0	
10	0	0	0	0	0.00	0	0	0	
11	0	0	0	0	0.00	0	0	0	
12	0	0	0	0	0.00	0	0	0	
13	0	0	0	0	0.00	0	0	0	
14	0	0	0	0	0.00	0	0	0	
15	0	0	0	0	0.00	0	0	0	
16	0	0	0	0	0.00	0	0	0	
17	0	0	0	0	0.00	0	0	0	
18	0	0	0	0	0.00	0	0	0	
19	0	0	0	0	0.00	0	0	0	
20	0	0	0	0	0.00	0	0	0	
21	0	0	0	0	0.00	0	0	0	

Refresh Save to File Close Reset Help

- 3 Do one of the following:
 - To refresh the statistics, click Refresh.
 - To close the statistics screen, click Close.

Network Statistics field descriptions

Column	Description
Hour	Identifies the hour that the statistics on that line apply to. These numbers refer to the most recent 24 hours, such that "1" refers to one hour ago, "2" refers to two hours ago, and so on.

Column	Description
Tx Frames	Identifies the number of frames transmitted in the given hour.
Rx Frames	Identifies the number of frames received in the given hour.
Rx Error	Identifies the number of frames received in the given hour with an error.
Rx Dropped	Identifies the number of received frames that the Remote Office system dropped in the given hour.
Error %	Identifies the percentage of frames received in the given hour with an error.
BroadCast Packet	Identifies the number of packets broadcast, or sent to all addresses on the network, by this unit in the given hour.
Tx UCastPkt	Identifies the number of packets unicast, or sent to one specific address, by this unit in the given hour.
Tx DiscPkt	Identifies the number of packets discarded by this unit in the given hour.
Rx MultiPkt	Identifies the number of packets received by this unit that were sent to multiple addresses in the given hour.
Rx UCastPkt	Identifies the number of packets received by this unit that were sent only to this unit in the given hour.
Rx DiscPkt	Identifies the number of received packets that were discarded by this unit in the given hour.

Section D: Performing upgrades

In this section

Verifying the firmware and software version	310
Obtaining the latest upgrade file	312
Extracting upgrade files from the download file	313
Performing a firmware upgrade	315
Performing a software upgrade	320

Verifying the firmware and software version

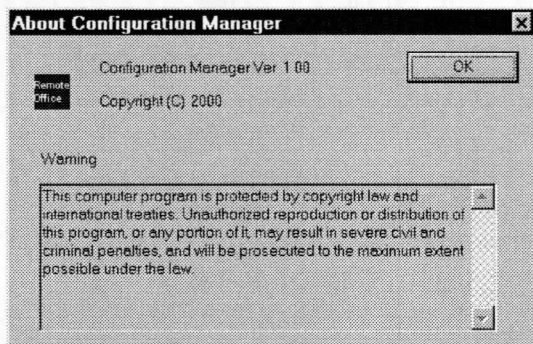
This section describes how to determine the version of firmware and software currently installed.

Before you perform a firmware or software upgrade, you should determine what version is currently installed. This ensures that you do not replace the installed firmware or software with an older version.

To verify the software version

From the menu, choose Help → About Configuration Manager.

Result: The following dialog box appears:



To verify the firmware version

- 1 From the menu, choose System Information → System Data.
- 2 The System Configuration Details screen appears.

System Configuration Details

Unit Id	254	Site Name	ALPHA_RLC
Unit Type	RLC-SINGLE WIDE	Unit Version	1_03_001.1 RLC
Database Version	1.19	Date	MAR-06-2001
		Time	14:24
IP Address	192.168.143.253	Mac Address	00:50:D7:04:5C:A3

Application Module Information

SLOTNO	STATUS	TYPE	VERSION
1	HEALTHY	DSP_2TMS320LC549	
2	HEALTHY	DSP_2TMS320LC549	
3	HEALTHY	DSP_2TMS320LC549	
4	HEALTHY	DSP_2TMS320LC549	

Successfully Read System Configuration Data

Close Help

- 3 Review the Firmware Version box. This identifies the version of firmware installed on the unit.

To determine the current firmware and software versions

To determine the current firmware and software versions, refer to the *Remote Office and RLC Release Notes* (NTP 555-8421-102).

Obtaining the latest upgrade file

If you need to upgrade the firmware or software, you can obtain the latest upgrade files by clicking on the Customer Support and Software Distribution links at the following website:

www.nortelnetworks.com

Nortel Networks provides upgrade files in self-extracting executable files. You must extract the upgrade files before you can perform the upgrade.

Types of upgrades

There are two types of upgrades that can be performed for your Remote Office 9150 unit:

- Configuration Manager software upgrade
- firmware upgrades
 - Remote Office 9150 motherboard firmware

Note: This includes any firmware updates that have been made for DSP application modules.
 - trunk interface module firmware

The firmware contains the code necessary for operating the Remote Office 9150 unit.

To download the upgrade file

- 1 With your web browser, connect to the Nortel Networks web site at <http://www.nortelnetworks.com/remotefice>.
- 2 Locate the software and firmware you need.
- 3 Download the files into a temporary location on your PC.
- 4 Extract the files into a temporary location on your PC by double-clicking the .exe file.
- 5 Continue with "Extracting upgrade files from the download file" on page 313.

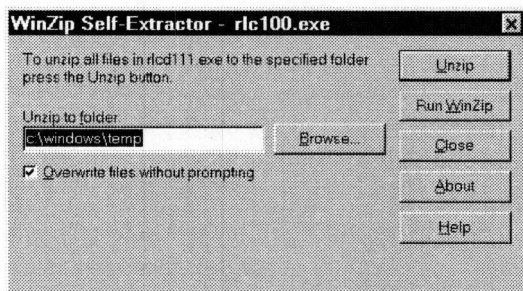
Extracting upgrade files from the download file

Before you perform an upgrade, ensure you have obtained the latest upgrade files from your Nortel Networks distributor. The upgrade files are enclosed in self-extracting executable files. You must extract the upgrade files before you can perform the upgrade.

To perform the extraction using Windows

- 1 Use Windows Explorer to navigate to the directory that contains the .exe file you received from Nortel Networks.
- 2 Locate and double-click the .exe file.

Result: The WinZip Self-Extractor screen similar to the following opens.



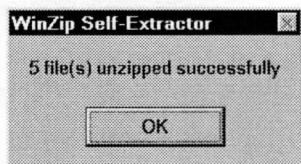
- 3 Review the information presented and make changes as necessary.

Notes:

- It is recommended that you extract the files into a temporary directory.
- If you specify a directory that does not exist, the WinZip Self-Extractor creates it.

- 4 Click Unzip.

Result: The file extraction begins. A status bar shows the extraction progress. When completed, a message similar to the following appears:



- 5 Click OK.

Result: The WinZip Self-Extractor screen reappears.

- 6 Click Close.

Performing a firmware upgrade

This section describes how to perform a firmware upgrade on your Remote Office 9150 unit. You perform the upgrade over the IP network using the TFTP protocol.

You must have a TFTP server application running on the administration PC. The TFTP server's base directory must point to the directory that contains the upgrade files.

To ensure that the RLC and Remote Office 9150 unit do not experience communication problems during or after the firmware upgrade, Nortel Networks recommends that you perform the upgrades in the steps shown below.

1. Create backup files for the Remote Office 9150 unit and RLC configurations. Refer to "Creating a backup configuration file" on page 266.
2. Upgrade the Configuration Manager software.
3. Disable the slot in which the RLC is installed.
4. Upgrade the RLC firmware.
5. Upgrade the Remote Office 9150 unit firmware.
6. Upgrade the BRI module firmware for each BRI module on your Remote Office 9150 units.
7. Restart both units.
8. Re-enable the RLC slot.

When to perform a firmware upgrade

Perform a firmware upgrade if you have determined that you are using out-of-date firmware. For instructions on determining if you need to perform an upgrade, see “Verifying the firmware and software version” on page 310.



CAUTION

Risk of incorrect operation

You must ensure that the RLC's firmware has been upgraded before you upgrade the Remote Office 9150 unit's firmware. This ensures that communication problems between the RLC and Remote Office 9150 unit do not occur.

About firmware upgrades and configuration files

Each time you perform a firmware upgrade, the configuration database is also converted (if necessary) to a format that is compatible with the new firmware. Configuration settings are not affected by the conversion.

Nortel Networks recommends that, each time you perform a firmware upgrade, you create a backup copy of the converted configuration file, and store it in a safe secure location.

Before you begin

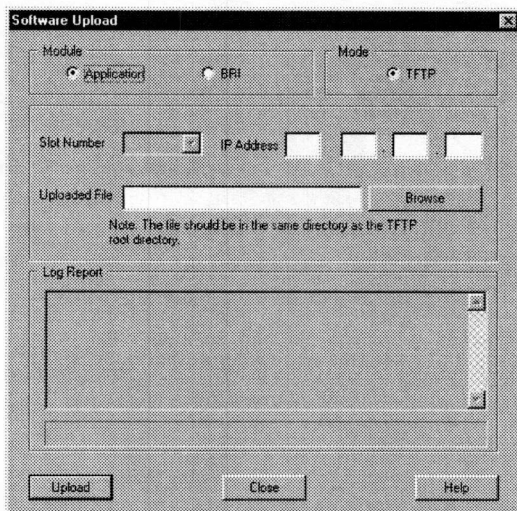
- 1 Obtain the firmware upgrade from Nortel Networks.
For instructions, see “Obtaining the latest upgrade file” on page 312.
- 2 Extract the upgrade files from the file you received from Nortel Networks.
For instructions, see “Extracting upgrade files from the download file” on page 313.
- 3 Start the TFTP server application.
- 4 Ensure the TFTP base directory reflects the directory where the firmware upgrade file you want to use is located.

Getting there 9150→ Configuration Manager

To upgrade the firmware

- 1 From the menu, choose Upload/Download → Upload S/W.

Result: The Software Upload screen appears.



- 2 Do one of the following:

IF you are upgrading THEN

motherboard firmware in the Module section, click Application.

ISDN BRI module do the following:

firmware

a In the Module section, click ISDN.

b Enter the position on the motherboard where the ISDN BRI module is installed.

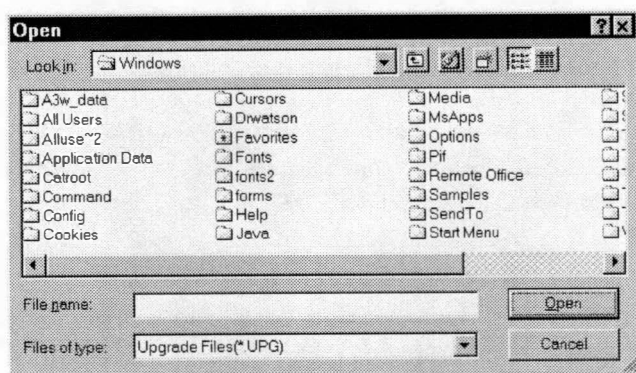
Valid values: 4 through 7

- 3 Enter the IP address of the TFTP server into the IP Address boxes.

Note: Since the TFTP server application is running on your administration PC, this is the IP address of the PC.

- 4 Click Browse.

Result: The Open dialog box appears.



- 5 Ensure the "Files of type" box shows Upgrade Files(*.UPG).
- 6 Navigate to the folder where the firmware file is located.

- 7 Select the file, and then click Open.

Examples:

- For motherboard firmware, select 9150-100.upg, and then click Open.
- For ISDN BRI module firmware, select briv15u.upg, and then click Open.

Result: You return to the Software Upload dialog box. The file you selected is shown in the Uploaded File box.

- 8 Click Upload.

Wait until the file uploads completely before entering any other commands. The Log Report box displays a confirmation message when the upgrade is completed.

- 9 Restart the Remote Office 9150 unit.

Performing a software upgrade

Perform a software upgrade if you have determined that you are using out-of-date software. For instructions on determining if you need to perform an upgrade, see “Verifying the firmware and software version” on page 310.

To upgrade the Configuration Manager software

- 1 Use Windows Explorer to navigate to the directory that contains the upgrade files you extracted.
- 2 Locate and double-click the setup.exe file.
- 3 Follow the prompts on the screen.

ATTENTION

Do not ignore any warning messages that the InstallShield displays about versions of files (such as DLL files) that already exist on your PC. If you overwrite these files, you can inadvertently cause other applications on your PC to stop working.

Result: The InstallShield installs the software on top of the previous version.

Chapter 8

Troubleshooting

In this chapter

Before you begin	322
Remote Office 9150 LEDs	323
Digital telephone	325
Device connectivity	330
Software problems	334
Using Configuration Manager's Ping	336
Recovering from a catastrophic failure	339

Before you begin

If you experience problems in setting up or running your Remote Office 9150 unit, this chapter will help you to isolate and solve the problem.

Identifying why the problem occurred

Before you begin, ask yourself the questions listed in the following table:

Question	IF you answered	THEN do the following:
Is this a new installation?	yes	Perform troubleshooting in the sequence presented in this chapter.
	no	Answer the next question.
Did the Remote Office 9150 unit work, and then suddenly stop working?	yes	Answer the next question.
	no	Perform troubleshooting in the sequence presented in this chapter.
Did you modify the configuration or change any hardware components?	yes	1 Verify that changes were done correctly. 2 Check the hardware components to ensure they are in working order. 3 Perform troubleshooting for the specific component.
	no	Contact your telecom or data network administrator. There might be a problem with the network.

Remote Office 9150 LEDs

During a Remote Office 9150 unit power-up cycle, watch the front panel of the Remote Office 9150 unit. The LEDs should appear as follows:

- The Power LED should light and remain lit.
- The Status LED should stay lit after the power-up cycle is completed. When the Status LED is lit all the time, the unit is healthy.
- The remaining LEDs flash whenever there is network activity.

What to do if the LEDs do not display correctly

The following table describes what to do if the LEDs do not display correctly:

Symptom	What to do
The Status LED is not lit.	1 Did the Status LED ever illuminate? If not, contact your Nortel Networks distributor. There might be a hardware problem. 2 Are other LEDs lit or flashing? If no, ensure the power cable is connected to both the power source and the Remote Office 9150 unit. If it has become disconnected, reconnect it. 3 If the Status LED is still out, contact your Nortel Networks distributor. There might be a hardware problem.
No LEDs are lit on the Remote Office 9150 unit.	1 Ensure that the Remote Office 9150 unit is connected to a power source. 2 If you are using an uninterruptible power supply (UPS), ensure the UPS is powered on. 3 Verify that the AC power source is operational.

Symptom	What to do
The Ethernet COLL LED is lit solid.	Network collisions are bound to occur and are normal. However, if this LED is lit solid, do the following: 1 Check the physical network connection. 2 Verify that the Remote Office 9150 unit can be pinged. 3 Check the network configuration (such as routing, traffic load, and so on). Adjust the network configuration, if required. 4 There should be no broadcast or multicast activity on the telephony LAN (TLAN). Interconnect a hub and a network analyzer to the TLAN and monitor for such activity. Identify the source(s) and isolate them from the TLAN.

Digital telephone

This section identifies some problems that could occur on the digital telephone, and describes what to do to resolve them.

Symptom descriptions

If you are having trouble with digital telephones, perform troubleshooting as described in the following table:

Symptom	What to do
There is no dial tone when pressing either the host call appearance or local call appearance keys.	1 Is this a first-time installation? If yes, perform troubleshooting as described in “What to do if the telephone connection tests do not work” on page 140. 2 If you are trying to make a host-controlled call, check the IP network and ensure that ■ it is not down ■ traffic is being routed between the Remote Office 9150 unit and RLC on the host PBX 3 If you are trying to make a host- or locally controlled call, Ensure the ISDN BRI line is working. Ask your service provider to check this. 4 Restart the RLC, wait one minute, and then restart the Remote Office 9150 unit. 5 Ensure the RLC is enabled in its host PBX slot. In Load 97 on the Meridian 1 PBX, stat the RLC, disable and enable it, or reseal it if necessary.

Symptom	What to do
There is no dial tone when pressing either the host call appearance or local call appearance keys. (continued)	6 Contact your telecom administrator. There might be problems at the host PBX.
Lamps or indicators are not lit after completion of a Remote Office 9150 unit power cycle.	1 Check all cable connections to and from the Remote Office 9150 unit and ensure they are all securely connected. 2 Is this a first-time installation? If yes, check the telephone connections. Refer to the Telco 1 and Telco 2 cable pin-out tables in Appendix C, "Connection pin-out tables." 3 Ensure the ISDN BRI line is working. Ask your service provider to check this. 4 Check the IP network and ensure that ■ it is not down ■ traffic is being routed between the Remote Office 9150 unit and RLC on the host PBX 5 Ping the RLC from the Remote Office 9150 unit to verify IP network connectivity.
Lamps or indicators do not reflect the true status of the telephone.	It is possible that there is a synchronization error between the Remote Office 9150 unit and the host PBX. Contact your telecom network administrator.
The display is blank (that is, the time and date are not displayed).	1 Take the digital telephone handset off hook and dial the Online SPRE code. The Remote Office 9150 unit attempts to connect to the host PBX. When the connection is established, the time and date appear.

Symptom	What to do
The display is blank (that is, the time and date are not displayed). (continued)	2 Check the IP network and ensure that ■ it is not down ■ traffic is being routed between the Remote Office 9150 unit and RLC on the host PBX 3 Ping the RLC from the Remote Office 9150 unit to verify IP network connectivity. 4 Ensure the ISDN BRI line is working. Ask your service provider to check this. 5 Restart the RLC, wait one minute, and then restart the Remote Office 9150 unit. 6 Ensure the RLC is enabled in its host PBX slot. In Load 97 on the Meridian 1 PBX, stat the RLC, disable and enable it, or reseal it if necessary. 7 Contact your telecom administrator. There might be problems at the host PBX.
There are noticeable gaps or poor quality when a voice call is active on the IP network.	1 Check the Quality of Service configuration on the RLC. Adjust the configuration, if required. Lower the QoS threshold so that transition occurs earlier. 2 Conduct a traffic study on your voice and IP network traffic patterns as described in the <i>Remote Office Network Engineering Guidelines</i> (555-8421-230). It is possible that your IP network capacity cannot accommodate the additional voice data, especially during High Day Busy Hour (HDBH) periods. Make adjustments to your network as required.

Symptom	What to do
Incoming calls are not being received from the host PBX.	1 Ensure your telephone is not on call forward. 2 Ensure the Remote Office 9150 unit is not in offline mode by entering the Online SPRE code at a digital telephone. 3 Ensure the Remote Office 9150 unit is powered up. It cannot receive calls from the host PBX if it is not powered up. 4 Ensure the RLC is correctly configured with your Remote Office 9150 unit's IP address, telephone number, and security ID (if they are used). 5 Ensure the ISDN BRI line is working, if it is being used to route host-controlled calls. Ask your service provider to check this. 6 Check the IP network (if it is being used) and ensure that ■ it is not down ■ traffic is being routed between the Remote Office 9150 unit and RLC on the host PBX 7 Ping the RLC from the Remote Office 9150 unit to verify IP network connectivity. 8 If the problem persists, contact your telecom administrator or Nortel Networks distributor.
Incoming calls are not being received from the PSTN.	1 Ensure your telephone is not on call forward. 2 Ensure the calling party has your office's correct telephone number. 3 Ensure the Remote Office 9150 unit is powered up. It cannot receive calls from the host PBX or the PSTN if it is not powered up.

Symptom	What to do
Incoming calls are not being received from the PSTN. (continued)	4 Ensure the ISDN BRI line is working. Ask your service provider to check this. 5 If the problem persists, contact your telecom administrator or Nortel Networks distributor.
A call in progress was suddenly disconnected.	1 Does your telephone display "Offline Mode?" If so, enter the Online SPRE code to go back online. 2 Contact your telecom and data network administrators. Perhaps network problems caused the call to drop.

Device connectivity

This section identifies some problems that can occur on the data network, and describes what to do to resolve them.

Symptom descriptions

If you are not able to establish or maintain data network connectivity, perform troubleshooting as described in the following table.

Note: To enable valid loopback testing of serial ports and cables, Nortel Networks recommends that you use a breakout box.

Symptom	What to do
SERIAL CONNECTION FAILED appears when attempting to connect to the Remote Office 9150 unit.	1 Ensure that you entered the logon ID and password correctly when trying to establish the connection. 2 Ensure that someone else is not already logged on to the Remote Office 9150 unit. 3 Ensure that you selected the correct COM port when trying to establish the connection. 4 Verify that no other applications on the administration PC are using the COM port. 5 Verify that the serial connection is good. 6 Using a breakout box, verify that the COM port is active. 7 Ensure the Remote Office 9150 unit is powered up. 8 Power the Remote Office 9150 unit off, and then back on. 9 Contact your Nortel Networks distributor. There might be a hardware problem.

Symptom

10060 TELNET CONNECTION FAILED appears when attempting to connect to the Remote Office 9150 unit.

What to do

- 1 Ensure that you entered the logon ID and password correctly when trying to establish the connection.
- 2 Ensure that you entered the IP address correctly when trying to establish the connection.
- 3 Ensure that someone else is not already logged on to the Remote Office 9150 unit.
- 4 Verify that the Ethernet cable is connected at both ends (the Remote Office 9150 unit and the network hub).
- 5 Check the Ethernet cable and ensure it is good.
- 6 Ensure the Remote Office 9150 unit is powered up.
- 7 Power the Remote Office 9150 unit off, and then back on.
- 8 Ensure the Remote Office 9150 unit's IP address, network mask, and default gateway are correctly configured in the Remote Office 9150 unit.
- 9 Ping the Remote Office 9150 unit to see if it responds.
- 10 If the Remote Office 9150 unit does not respond, ping the Remote Office 9150 unit's gateway to see if it responds.
- 11 If the gateway does not respond, ping a known good device on the Remote Office 9150 unit's network.
- 12 If steps 10 and 11 work, but step 9 did not, there might be a gateway configuration error. Contact your data network administrator.
- 13 Contact your Nortel Networks distributor. There might be a hardware problem.

Symptom	What to do
There are many collisions on the Ethernet network, as indicated by a solid Ethernet COLL LED.	Network collisions are bound to occur and are normal. However, if this LED is lit solid, do the following: 1 Check the physical network connection. 2 Verify that the Remote Office 9150 unit can be pinged. 3 Check the network configuration (such as routing, traffic load, and so on). Adjust the network configuration, if required. 4 There should be no broadcast or multicast activity on the TLAN. Interconnect a hub and a network analyzer to the TLAN and monitor for such activity. Identify the source(s) and isolate them from the TLAN.
The Remote Office 9150 unit will not send or receive Ethernet traffic.	1 Ensure that the Remote Office 9150 unit is powered up. The Remote Office 9150 unit cannot send or receive traffic if it is not powered up. 2 Check the Ethernet cable between the Remote Office 9150 unit and the network, and ensure that it is good. 3 Ensure the Ethernet cable is connected. 4 If the Remote Office 9150 unit still will not send or receive traffic, contact your data network administrator. 5 Data network administrator: Ensure that other network devices are configured to allow traffic to and from the Remote Office 9150 unit.
An attempt to log off from the Remote Office 9150 unit does not work.	It is possible that communication has been lost between the administration PC and the Remote Office 9150 unit. Close Configuration Manager, and then restart it.

Symptom	What to do
The Remote Office 9150 unit cannot establish a connection with the RLC.	1 Verify security authentication configuration and ensure that it matches at both ends. (For example, if the security identifier security level is used, ensure that the inbound and outbound security identifiers are correctly configured at each end.) 2 Ensure that the unit IDs have been correctly configured at each end. An incorrect unit ID causes security authentication to fail. 3 Ensure that the RLC's IP address and PSTN number are correctly configured on the Remote Office 9150 unit (as appropriate). 4 Verify that the IP network and PSTN are operational (up and running) as appropriate. 5 Ensure that the RLC is enabled on the host PBX. 6 Use the Ping option in Configuration Manager to ping the RLC. For instructions, see "Using Configuration Manager's Ping" on page 336. 7 If the RLC does not respond, check the network configuration (such as, routing, traffic load, and so on). Adjust the network configuration, if required.

Software problems

This section identifies some problems that can occur with the Configuration Manager software, and describes what to do to resolve them.

Symptom descriptions

If you are not able to complete a task with Configuration Manager, then perform troubleshooting as described in the following table:

Symptom	What to do
The Configuration Manager software installation fails.	Ensure that you close all background applications, including anti-virus checking software before performing the installation.
When performing one of the following by TFTP, ERROR: FILE OPEN FAILED appears: ■ configuration upload ■ firmware upgrade	1 Ensure the TFTP server application is installed and running on your administration PC. 2 Ensure the file you are trying to upload is present in the target directory. That is, either in the TFTP directory, or in the directory that is specified as the base directory in the TFTP server application. 3 Review messages displayed by the TFTP server application for clues. 4 Ping the Remote Office 9150 unit to verify that network connectivity exists.
CONFIG UPLOAD FAILED when attempting to perform a configuration upload by TFTP.	1 Ensure that you selected an appropriate file. That is, ensure that the file you attempted to upload is a Remote Office 9150 configuration file.

Symptom	What to do
CONFIG UPLOAD FAILED when attempting to perform a configuration upload by TFTP. (continued)	2 Ensure that the configuration file you are attempting to upload is compatible with current firmware. Perform the configuration upload using a previous configuration file, if necessary. Note: Each time you perform a firmware upgrade, you should also create a backup of the configuration. The configuration database format in the Remote Office 9150 unit is dependent on the version of firmware installed. If you recently downgraded to a previous version of firmware, you might also need to revert to a previous configuration format.
System not responding appears when working with Configuration Manager.	It is possible that communication has been lost between the administration PC and the Remote Office 9150 unit. Close Configuration Manager, and then restart it.
Nothing happens when attempting to log off from the Remote Office 9150 unit.	It is possible that communication has been lost between the administration PC and the node to which you were logged on. Close Configuration Manager, and then restart it.

Using Configuration Manager's Ping

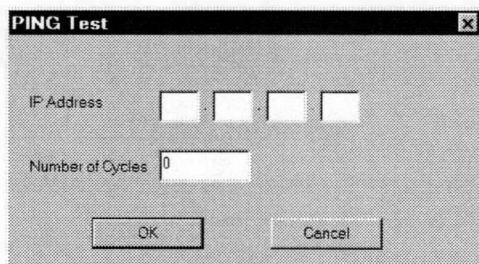
This section explains how to use the Ping option provided in Configuration Manager to verify network connectivity. Use this test as a troubleshooting tool to determine if you can reach the RLC, another remote unit, or any other device on the network.

Getting there 9150 → Configuration Manager

To perform a Configuration Manager ping

- 1 From the menu, choose Tests → Ping.

Result: The PING Test dialog box appears.

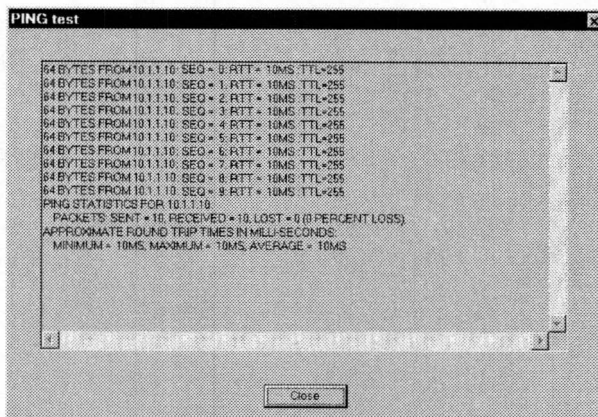


- 2 Enter the IP Address of the unit you want to ping.
- 3 In the Number of Cycles box, enter the number of times you want to ping the unit.

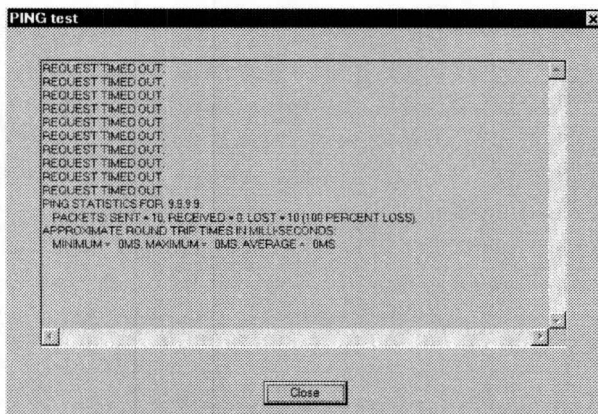
The number must be in the range of 1–100.

4 Click OK.

Result: The PING test results screen appears, showing the ping results. The following is an example of a successful ping:



The following is an example of an unsuccessful ping:



5 Click Close.

Result: The Ping test screen closes.

What to do if the ping did not work

- 1 Ensure that you entered the IP address correctly.
- 2 Ensure that the subnet mask and default gateway are properly configured on the device you are pinging.
Confirm this by viewing the IP Configuration property sheet for the device.
- 3 Ping the device's gateway.
- 4 If the gateway does not respond, ping a known good device on the device's network.
- 5 Contact your data network administrator. There may be a configuration error elsewhere on the network.

Recovering from a catastrophic failure

For the purposes of this discussion, a *catastrophic failure* is defined as a failure of the equipment to operate.

Inoperative hardware

If your Remote Office 9150 unit fails to operate, consult with your Nortel Networks distributor for hardware replacement.

Appendix A

Planning forms

In this appendix

Overview	342
Completing the Remote Office 9150 forms	344

Overview

This appendix provides several forms that you can use to plan and record the various data necessary for proper configuration of a Remote Office 9150 unit at your site.

Note: RLC forms are provided in the *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210).

Network planning

To help you plan your Remote Office network, study the network diagram and sample configurations provided in Appendix B, “Sample configuration files.” The information provided in this appendix demonstrates the relationships between RLC and Remote Office 9150 configuration settings.

Remote Office 9150 forms

Use the Remote Office 9150 forms to record information and calculate needed resources for a Remote Office 9150 unit. For more information about using these forms, see “Planning the configuration” on page 87.

Data entry form completion sequence

Information from some forms might need to be copied to other forms. Generally, you should complete the data entry forms in the following sequence:

1. Remote Office 9150 Configuration Information—Stations form
2. Reach Line Card Connection Information (for either the 16-port or 32-port RLC)
3. Remote Office 9150 Configuration Information—Network Connections form
4. Remote Office 9150 Configuration Information—ISDN BRI Modules form
5. Remote Office 9150 Configuration Information—Dialing Plans form

6. Reach Line Card Online/Offline Table Configuration (if required)

For more details, see “Completing the Remote Office 9150 forms” on page 344.

Completing the Remote Office 9150 forms

This section briefly describes how to complete the Remote Office 9150 configuration forms.

To complete the forms

- 1 Assign each user telephone or fax machine to a port on the Remote Office 9150 unit.

Record the assignments on the Remote Office 9150 Configuration Information—Stations form. Designate each port as a local port, remote port, or local and remote port.

- 2 Use the information you received from the ISDN service provider for the Remote Office 9150 site to complete the Remote Office 9150 Configuration Information—ISDN BRI Modules form.

At the same time, do the following:

- a. Designate a B-channel as a primary trunk. The Remote Office 9150 unit uses primary trunk to establish connections between the Remote Office 9150 unit and the RLC.

Note: The primary trunk on the Remote Office 9150 unit is defined as follows:

- the lowest-numbered B-channel defined as Remote only
- the lowest-numbered B-channel defined as Local and Remote

Do not include the primary trunk in any trunk groups. Nortel Networks recommends that you define the primary trunk as Remote only.

Record the primary trunk assignment in the "Connection to RLC information" section on the Remote Office 9150 Configuration Information—Network Connections form.

- b. Assign B-channels to trunk groups. Record the assignments on the ISDN BRI Modules form.

- 3 Assign an IP address, subnet mask, and gateway to the Remote Office 9150 unit. This information is required if you want to administer the Remote Office 9150 unit over the IP network.

Record the addresses in the "Remote Office 9150 unit identification" section on the Remote Office 9150 Configuration Information—Network Connections form.

- 4 If the security level chosen is security code, record the security identifier assigned to the Remote Office 9150 unit.
- 5 In the "Connection to RLC information" section on the Remote Office 9150 Configuration Information—Network Connections form, record the RLC's
 - IP address
 - telephone number
 - security code

The Remote Office 9150 unit uses this information to establish and authenticate connections with the RLC.

- 6 If an online/offline table is configured on the RLC, configure the SPRE codes for toggling the online/offline modes on the Remote Office 9150 unit.

Note: This step is optional, because default SPRE codes have already been defined in the software (as indicated on the Remote Office 9150 Configuration Information—Dialing Plans form).

If you choose to change the code, record the new code on the Dialing Plans form.

- 7 Define the trunk access and Paging SPRE codes.

Trunk access codes are used by Remote Office 9150 unit users to get outside lines.

Note: Default trunk access digits and paging SPRE codes have already been defined. Nortel Networks recommends that you use the defaults.

If you choose to change the predefined codes, record them on the Remote Office 9150 Configuration Information—Dialing Plans form. Also, record the trunk access codes (as required) on the ISDN BRI Modules form.

Remote Office 9150

Configuration Information—Stations

Page 1 of 4

Notes:

- A maximum of seven MCAs and ATAs can be connected to digital telephones at this site.
- If you are connecting a fax machine or analog device that is not equipped with an ATA, it can be connected only to port 64. If you want to connect a fax machine or analog device to any other port, it must be equipped with an ATA.

9150 port #	Extension number (DN)	Type			If a remote port, host port number (TN)	MCA or ATA?	
0		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
1		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
2		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
3		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
4		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
5		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
6		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
7		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
8		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
9		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
10		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
11		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
12		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
13		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
14		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
15		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
16		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
17		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
18		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No

Remote Office 9150

Configuration Information—Stations

Page 2 of 4

Notes:

- A maximum of seven MCAs and ATAs can be connected to digital telephones at this site.
- If you are connecting a fax machine or analog device that is not equipped with an ATA, it can be connected only to port 64. If you want to connect a fax machine or analog device to any other port, it must be equipped with an ATA.

9150 port #	Extension number (DN)	Type			If a remote port, host port number (TN)	MCA or ATA?	
19		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
20		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
21		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
22		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
23		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
24		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
25		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
26		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
27		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
28		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
29		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
30		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
31		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No

Use ports 32 through 63 only if this Remote Office 9150 unit connects to a 2-slot RLC on the host PBX.

32		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
33		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
34		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
35		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No

Remote Office 9150

Configuration Information—Stations

Page 3 of 4

Notes:

- A maximum of seven MCAs and ATAs can be connected to digital telephones at this site.
- If you are connecting a fax machine or analog device that is not equipped with an ATA, it can be connected only to port 64. If you want to connect a fax machine or analog device to any other port, it must be equipped with an ATA.

9150 port #	Extension number (DN)	Type			If a remote port, host port number (TN)	MCA or ATA?	
36		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
37		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
38		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
39		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
40		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
41		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
42		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
43		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
44		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
45		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
46		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
47		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
48		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
49		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
50		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
51		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
52		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
53		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No

Remote Office 9150

Configuration Information—Stations

Page 4 of 4

Notes:

- A maximum of seven MCAs and ATAs can be connected to digital telephones at this site.
- If you are connecting a fax machine or analog device that is not equipped with an ATA, it can be connected only to port 64. If you want to connect a fax machine or analog device to any other port, it must be equipped with an ATA.

9150 port #	Extension number (DN)	Type			If a remote port, host port number (TN)	MCA or ATA?	
54		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
55		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
56		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
57		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
58		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
59		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
60		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
61		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
62		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
63		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No
64: FAX		☐ Local	☐ Remote	☐ Both		☐ Yes	☐ No

Remote Office 9150

Configuration Information—ISDN BRI Modules

Page 1 of 3

Module 4

ISDN line type (variant): _____	Switch type: _____
B-channel 1 DN: _____	SPID: _____
	Connection type: ☐ Local ☐ Local and Remote ☐ Remote
Trunk group: _____	Trunk access code: _____
B-channel 2 DN: _____	SPID: _____
	Connection type: ☐ Local ☐ Local and Remote ☐ Remote
Trunk group: _____	Trunk access code: _____

Module 5

ISDN line type (variant): _____	Switch type: _____
B-channel 1 DN: _____	SPID: _____
	Connection type: ☐ Local ☐ Local and Remote ☐ Remote
Trunk group: _____	Trunk access code: _____

Remote Office 9150

Configuration Information—ISDN BRI Modules

Page 2 of 3

Module 5 (continued)

B-channel 2 DN: _____	SPID: _____
	Connection type: ☐ Local ☐ Local and Remote ☐ Remote
Trunk group: _____	Trunk access code: _____

Module 6

ISDN line type (variant): _____	Switch type: _____
B-channel 1 DN: _____	SPID: _____
	Connection type: ☐ Local ☐ Local and Remote ☐ Remote
Trunk group: _____	Trunk access code: _____
B-channel 2 DN: _____	SPID: _____
	Connection type: ☐ Local ☐ Local and Remote ☐ Remote
Trunk group: _____	Trunk access code: _____

Remote Office 9150

Configuration Information—ISDN BRI Modules

Page 3 of 3

Module 7

ISDN line type (variant): _____	Switch type: _____
B-channel 1 DN: _____	SPID: _____
Trunk group: _____	Connection type: ☐ Local ☐ Local and Remote ☐ Remote
B-channel 2 DN: _____	Trunk access code: _____
Trunk group: _____	SPID: _____
	Connection type: ☐ Local ☐ Local and Remote ☐ Remote
	Trunk access code: _____

Remote Office 9150

Configuration Information—Network Connections

Page 1 of 1

Security level: ☐ No security ☐ Caller ID ☐ Provision ID					
Remote Office 9150 unit identification					
Node number: _____	Node name: _____				
IP address:	<table border="1" style="width: 100%; height: 20px; border-collapse: collapse;"> <tr> <td style="width: 25%;"> </td><td style="width: 25%;"> </td><td style="width: 25%;"> </td><td style="width: 25%;"> </td> </tr> </table>				
Subnet mask:	<table border="1" style="width: 100%; height: 20px; border-collapse: collapse;"> <tr> <td style="width: 25%;"> </td><td style="width: 25%;"> </td><td style="width: 25%;"> </td><td style="width: 25%;"> </td> </tr> </table>				
Default gateway:	<table border="1" style="width: 100%; height: 20px; border-collapse: collapse;"> <tr> <td style="width: 25%;"> </td><td style="width: 25%;"> </td><td style="width: 25%;"> </td><td style="width: 25%;"> </td> </tr> </table>				
If the security level is Provision ID, what is the Remote Office 9150 unit's security identifier?					
Connection to RLC information					
IP address to reach the host PBX (for IP network):					
<table border="1" style="width: 100%; height: 20px; border-collapse: collapse;"> <tr> <td style="width: 25%;"> </td><td style="width: 25%;"> </td><td style="width: 25%;"> </td><td style="width: 25%;"> </td> </tr> </table>					
Telephone number to reach host PBX (for PSTN):					
If security level is Provision ID, what is the RLC's security identifier?					
Trunk dedicated as the primary trunk:					
Note: Refer to the Remote Office 9150 Configuration Information—ISDN BRI Modules form.					
Module:	☐ 4 ☐ 5 ☐ 6 ☐ 7				
B-channel	☐ 1 ☐ 2				

Remote Office 9150

Configuration Information—Dialing Plans

Page 1 of 1

Notes:

- Nortel Networks recommends that you use the preconfigured default codes listed below.
- The pound sign (# in North America) is mandatory and is automatically preconfigured in Configuration Manager. The pound sign prevents conflicts with the dialing plan on the host PBX.
- You can dedicate all B-channels to one trunk group. You do not have to create a trunk group for each B-channel.

Description	Default code	Your code (maximum of 3 digits)
Online SPRE code	#99	#
Offline SPRE code	#98	#
Paging SPRE code	#05	#
Local Calling SPRE code (for analog or ATA-equipped stations)	#8	#
Registration SPRE code (for multi-user or dynamic pool ports only)	#97	#
Deregistration SPRE code (for multi-user or dynamic pool ports only)	#96	#
Access code for trunk group 1	#61	#
Access code for trunk group 2	#62	#
Access code for trunk group 3	#63	#
Access code for trunk group 4	#64	#
Access code for trunk group 5	#65	#
Access code for trunk group 6	#66	#
Access code for trunk group 7	#67	#
Access code for trunk group 8	#68	#

Remote Office 9150

System expansion worksheet

Page 1 of 3

Complete one worksheet for each Remote Office 9150 unit.

Number of stations:

- 1 How many digital telephones will be installed at the Remote Office 9150 site?

Note: A maximum of 32 digital telephones can be connected to the Remote Office 9150 unit.

- 2 How many Analog Telephone Adapters (ATAs) will be installed?

- 3 How many Meridian Communication Adapters (MCAs) will be installed?

- 4 Add lines 1 and 2 together.

Notes:

- A maximum of four MCAs and ATAs can be installed when connecting the Remote Office 9150 unit to a 1-slot RLC. A maximum of seven MCAs and ATAs can be installed when connecting to a 2-slot RLC.

- The total number of ATAs and digital telephones cannot exceed 32.

- 5 Will a fax machine be used for faxes through the host PBX? ☐ Yes

☐ No

- 6 If line 5 is Yes, add 1 to line 4.

Call blocking:

- 7 Do you want to implement call blocking? (Users will receive a fast busy signal when resources are not available.) ☐ Yes

☐ No

- 8 If line 7 is Yes, calculate the number of calls that can be active at one time.

Note: A conservative estimate of one call in three being blocked when no resources are available is recommended.

Multiply line 4 by your call blocking factor. For example, to calculate the number of simultaneous calls that can be supported at a 3:2 blocking ratio, multiply line 6 by 2/3 (0.666). If the result contains a fraction, round up to a whole number.

Line 6: _____ x _____ = _____

If line 7 is No, the number of simultaneous calls is the same as the number of stations installed. (Record your response to line 6 here.) _____

Remote Office 9150

System expansion worksheet

Page 2 of 3

Call routing:

- 9 How do you want to route host-controlled calls?

☐ IP network ☐ Circuit-switched network ☐ Both

Note: If you want to route host-controlled calls over both networks, then the QoS transition technology can be used.

- 10 If line 9 is Circuit-switched network or Both, do you want to support local-controlled calls through the circuit-switched network (that is, support local calling)?

☐ Yes ☐ No

Number of trunk interface modules needed for QoS transition support or routing calls over the circuit-switched network:

Note: If you are routing calls over the IP network only, skip this section.

- 11 If line 10 is No, enter 0.

If line 10 is Yes, how many simultaneous digital telephone or ATA local calls do you want to support?

Enter a value between 1–7.

Note: Only one active call per ISDN BRI B-channel is allowed in local-controlled mode because local calls are not compressed.

- 12 Calculate the number of B-channels required for simultaneous calls in host-controlled mode.

Each B-channel can support one MCA call, or up to eight simultaneous voice calls using G.729A compression (where each call is compressed to 8 Kbps). However, when using G.729A compression, the first B-channel can support only six simultaneous calls because 16 Kbps are required for transporting call signaling data for the entire Remote Office 9150 unit (and all of its connected stations) to the host PBX.

Line 3: _____ + ((# of simultaneous calls: _____ * 8 Kbps) + 16 Kbps) / 64 = _____

Round up the result to a whole number.

Remote Office 9150

System expansion worksheet

Page 3 of 3

Number of trunk interface modules needed (continued):

- 13 Calculate the number of B-channels required for both local- and host-controlled calls. Add lines 11 and 12.

If the result is greater than 8, then call blocking must be implemented, or the number of simultaneous local calls must be reduced.

Recalculate lines 8, 11, 12, and 13. _____

- 14 Calculate the number of trunk interface modules required for local calls. Divide line 13 by 2. If the result contains a fraction, round it up to the next whole number.

Line 13: _____ / 2 = _____

- 15 How many trunk interface modules are already installed in the Remote Office 9150 unit? _____

- 16 Calculate the number of trunk interface modules you need to purchase. Subtract line 15 from line 14. _____

Note: A maximum of four trunk interface modules can be installed in the Remote Office 9150 unit.

Number of DSP application modules needed:

- 17 Each DSP application module can support up to eight simultaneous calls over the IP network.

Divide line 8 by 8, and then round up the result to a whole number.

Line 8: _____ / 8 = _____

- 18 Record the number of DSP application modules already installed.

Note: The Remote Office 9150 unit ships from Nortel Networks with one DSP module already installed. Your response here must include that module. _____

- 19 Calculate how many DSP modules you need to purchase.

Subtract line 18 from line 17.

Note: A maximum of three DSP application modules can be installed in the Remote Office 9150 unit. _____

Appendix B

Sample configuration files

In this appendix

Example of a network	360
Voice port configuration on the Meridian 1 PBX	362
Data port configuration on the Meridian 1 PBX	364
RLC configuration	366
Remote Office 9150 unit	370

Example of a network

This section provides an example of a network diagram that shows one host site (RLC installed on the host PBX) and one Remote Office 9150 unit (with one user station). The purpose of this diagram is to demonstrate the relationship between configuration settings on each unit in the network.

Sample configuration printouts

Sample Meridian 1 PBX configuration printouts for the voice and data ports are provided as follows:

- voice port: on page 362
- data port: on page 364

Sample configuration printouts for the RLC and Remote Office 9150 unit are shown as follows:

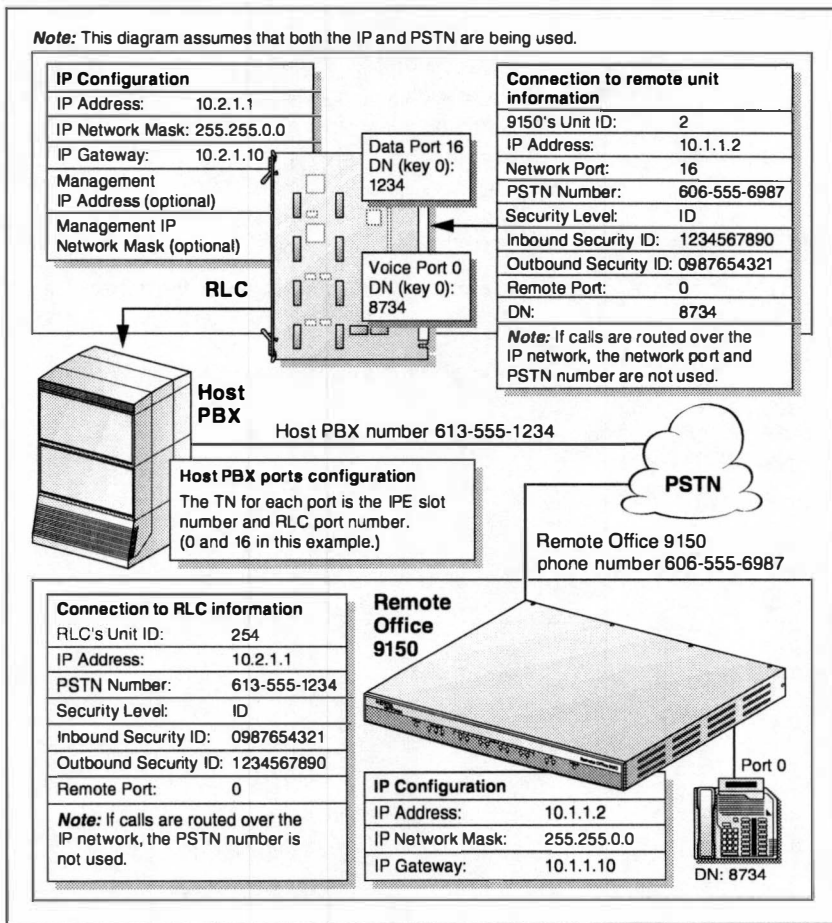
- RLC: on page 366
- Remote Office 9150 unit: on page 370

Configuration recommendation

The quickest way to configure the RLC and Remote Office 9150 unit is to run the Configuration Wizard. For instructions, see “Using the Configuration Wizard to perform initial configuration” on page 124. For your reference, the Configuration Wizard screen examples are completed using the same information.

Note: The network diagram shows information that cannot be configured through the Configuration Wizard, such as the security identifiers. You must use Configuration Manager to complete the configuration.

Network diagram



G101413

Voice port configuration on the Meridian 1 PBX

This section shows the configuration settings for the voice port on the Meridian 1 PBX. Generally, define voice ports according to the needs of your remote users.

Configuration example

This configuration example uses the settings identified in the network diagram shown on page 361.

Note: This configuration example is from a Meridian 1 Option 11.

```
REQ: prt
TYPE: 2616
MARF NOT ACTIVATED
TN 5 0
DATE
PAGE
DES
DES Bryan Dion
TN 005 0 00 00
TYPE 2616
CDEN 8D
CUST 0
AOM 0
FDN
TGAR 1
LDN NO
NCOS 0
SGRP 0
RNPG 0
SCI 0
SSU
XLST
```

← Telephone type

← RLC slot and port numbers

```

CLS   CTD FBD WTA LPR MTD FND HTD ADD HFD
      MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
      POD DSX VMD CMSD CCSD SWD LND CNDD
      CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBF
      ICDD CMDM LLCN MCTD CLBD AUTU
      GPUD DPUD DNDD CFXD ARHD CLTD ASCD
      CPFA CPTA ABDD CFHD FICD NAID BUZZ AHD
      DDGA NAMA
      DRDD EXR0
      USMD USRD ULAD RTDD RBDD RBHD PGND FLXD FTTC DNDY DNO3
CPND_LANG ENG
HUNT
PLEV 02
AST
IAPG 0
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
DNDR 0
KEY 00 SCR 8734 0      MARP
      CPND
      NAME Bryan Dion
      XPLN 24
      DISPLAY_FMT FIRST, LAST
01 CWT
02 MSB
03 TRN
04 CFW 4
05 AO6
06
07
08
09
10 MCR 8234 0 MARP
      CPND
      NAME Bryan Dion
      XPLN 24
      DISPLAY_FMT FIRST, LAST
11 AO6
12
13 DSP
14
15

```

VCE defines the port as a voice port.

9150 unit user's DN

9150 unit user's CPND

Data port configuration on the Meridian 1 PBX

This section shows the configuration settings for the data port on the Meridian 1 PBX. The data port provides the communication path between the RLC and the Remote Office 9150 unit, and must be configured as an MCA adapter.

Configuration example

This configuration example uses the settings identified in the network diagram shown on page 361.

Note: This configuration sample is from a Meridian 1 Option 11.

```

REQ: prt
TYPE: 2616
TN 5 16
DES
DES Remote site 1
TN 005 0 00 16
TYPE 2616
CDEN 8D
CUST 0
AOM 0
FDN
TGAR 1
LDN NO
NCOS 0
SGRP 0
RNPG 0
SCI 0
SSU
XLST
CLS CTD FBD WTD LPR MTD FND HTD ADD HFD
MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD DTA DRG1
POD DSX VMD CMSD CCSD SWD LND CNDD
CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBD
ICDD CDMD LLCN MCTD CLBD AUTU
GPUD DPUD DNDD CFXD ARHD CLTD ASCD
CPFA CPTA ABDD CFHD FICD NAID BUZZ AHD
DDGA NAMA
DRDD EXR0
USMD USRD ULAD RTDD RBDD RBHD PGND FLXD FTTC DNDY DNO3

```

← Telephone type

← RLC slot and port numbers

← TGAR must be configured to allow trunk access. Refer to your PBX documentation for more details.

DTA defines the port as a data port.

```
TOV 0 MINS
DTAO MCA
PSEL DMDM
HUNT
PSDS NO
TRAN ASYN
PAR SPACE
DTR ON
DUP FULL
HOT OFF
AUT ON
BAUD 9600
DCD ON
PRM KBD ON
VLL OFF
MOD YES
INT OFF
CLK OFF
KBD ON
RTS OFF
PLEV 02
AST
IAPG 0
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
DNDR 0
KEY 00 SCR 1234 0 MARP
01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
```

Network ports must be defined as MCA.

The number that the Remote Office 9150 unit needs to connect to the RLC. It must be a DID number.

RLC configuration

This section shows the configuration settings for the RLC. You can obtain a similar configuration printout by performing a configuration download while connected to the RLC.

Note: Configuration settings are separated by commas (,).

Configuration example

This configuration example uses the settings identified in the network diagram shown on page 361.

```
IPCFG 10.2.1.1,255.255.0.0,10.2.1.10,10.3.1.2,255.255.0.0
```

RLC's IP address information:

- IP address
- Subnet mask
- IP gateway
- Management IP address
- Management subnet mask

```
APPMODCFG 0,NC,NC
APPMODCFG 1,E,G729,G729
APPMODCFG 2,NC,NC
APPMODCFG 3,NC,NC
APPMODCFG 4,NC,NC
APPMODCFG 5,NC,NC
APPMODCFG 6,NC,NC
APPMODCFG 7,NC,NC
```

DSP application module
(only module 1 is configured
in this case)

```
SYSCFG 1,HOST1
```

Unit ID and node name

```
RLCCFG E,E
ACCFG D
```

```
PORTCFG 0,1,0,2,2,D
PORTCFG 1,1,0,2,2,D
PORTCFG 2,1,0,2,2,D
PORTCFG 3,1,0,2,2,D
PORTCFG 4,1,0,2,2,D
PORTCFG 5,1,0,2,2,D
```

Ports configured as remote ports


```

PORTCFG 6,0
PORTCFG 7,0
PORTCFG 8,0
PORTCFG 9,0
PORTCFG 10,0
PORTCFG 11,0
PORTCFG 12,0
PORTCFG 13,0
PORTCFG 14,0
PORTCFG 15,0

```

Ports configured as
local ports



```

PORTCFG 16,2,2,6065556987
PORTCFG 17,0
PORTCFG 18,0
PORTCFG 19,0
PORTCFG 20,0
PORTCFG 21,0
PORTCFG 22,0
PORTCFG 23,0
PORTCFG 24,0
PORTCFG 25,0
PORTCFG 26,0
PORTCFG 27,0

```

Port configured as
network port



```

.
.
.
PORTCFG 63,0

```

```

RUNITCFG 1,E,0,2,45,45,3,1234567890,0987654321,E,Y,10.1.1.2,
E,16,D,16,10,Y,6065556987,D

```

```

RUNITCFG 2,D,0,0,2,1,1,D,D,D
RUNITCFG 3,D,0,0,2,1,1,D,D,D
RUNITCFG 4,D,0,0,2,1,1,D,D,D
RUNITCFG 5,D,0,0,2,1,1,D,D,D
RUNITCFG 6,D,0,0,2,1,1,D,D,D
RUNITCFG 7,D,0,0,2,1,1,D,D,D
RUNITCFG 8,D,0,0,2,1,1,D,D,D
RUNITCFG 9,D,0,0,2,1,1,D,D,D
RUNITCFG 10,D,0,0,2,1,1,D,D,D

```

Remote unit connection
information (unit 1):



- remote unit number
- 9150's unit ID
- security information
(inbound and outbound
security IDs)
- remote unit's IP address
- network port
- PSTN number

```
ONOFFCFG 1,SUN,0 00:00
ONOFFCFG 1,MON,0 00:00
ONOFFCFG 1,TUE,0 00:00
ONOFFCFG 1,WED,0 00:00
ONOFFCFG 1,THU,0 00:00
ONOFFCFG 1,FRI,0 00:00
ONOFFCFG 1,SAT,0 00:00
ONOFFCFG 2,SUN,0 00:00
ONOFFCFG 2,MON,0 00:00
ONOFFCFG 2,TUE,0 00:00
ONOFFCFG 2,WED,0 00:00
ONOFFCFG 2,THU,0 00:00
ONOFFCFG 2,FRI,0 00:00
ONOFFCFG 2,SAT,0 00:00
ONOFFCFG 3,SUN,0 00:00
ONOFFCFG 3,MON,0 00:00
ONOFFCFG 3,TUE,0 00:00
ONOFFCFG 3,WED,0 00:00
ONOFFCFG 3,THU,0 00:00
ONOFFCFG 3,FRI,0 00:00
ONOFFCFG 3,SAT,0 00:00
ONOFFCFG 4,SUN,0 00:00
ONOFFCFG 4,MON,0 00:00
ONOFFCFG 4,TUE,0 00:00
ONOFFCFG 4,WED,0 00:00
ONOFFCFG 4,THU,0 00:00
ONOFFCFG 4,FRI,0 00:00
ONOFFCFG 4,SAT,0 00:00
ONOFFCFG 5,SUN,0 00:00
ONOFFCFG 5,MON,0 00:00
ONOFFCFG 5,TUE,0 00:00
ONOFFCFG 5,WED,0 00:00
ONOFFCFG 5,THU,0 00:00
ONOFFCFG 5,FRI,0 00:00
ONOFFCFG 5,SAT,0 00:00
ONOFFCFG 6,SUN,0 00:00
ONOFFCFG 6,MON,0 00:00
ONOFFCFG 6,TUE,0 00:00
ONOFFCFG 6,WED,0 00:00
ONOFFCFG 6,THU,0 00:00
ONOFFCFG 6,FRI,0 00:00
```

← Online/offline schedule

```
ONOFFCFG 6,SAT,0 00:00
ONOFFCFG 7,SUN,0 00:00
ONOFFCFG 7,MON,0 00:00
ONOFFCFG 7,TUE,0 00:00
ONOFFCFG 7,WED,0 00:00
ONOFFCFG 7,THU,0 00:00
ONOFFCFG 7,FRI,0 00:00
ONOFFCFG 7,SAT,0 00:00
ONOFFCFG 8,SUN,0 00:00
ONOFFCFG 8,MON,0 00:00
ONOFFCFG 8,TUE,0 00:00
ONOFFCFG 8,WED,0 00:00
ONOFFCFG 8,THU,0 00:00
ONOFFCFG 8,FRI,0 00:00
ONOFFCFG 8,SAT,0 00:00
ONOFFCFG 9,SUN,0 00:00
ONOFFCFG 9,MON,0 00:00
ONOFFCFG 9,TUE,0 00:00
ONOFFCFG 9,WED,0 00:00
ONOFFCFG 9,THU,0 00:00
ONOFFCFG 9,FRI,0 00:00
ONOFFCFG 9,SAT,0 00:00
ONOFFCFG 10,SUN,0 00:00
ONOFFCFG 10,MON,0 00:00
ONOFFCFG 10,TUE,0 00:00
ONOFFCFG 10,WED,0 00:00
ONOFFCFG 10,THU,0 00:00
ONOFFCFG 10,FRI,0 00:00
ONOFFCFG 10,SAT,0 00:00
```

```
FBQOSCFG 1,E,5,6,5,10,10,32
FBQOSCFG 2,D,5,6,5,10,10,32
FBQOSCFG 3,D,5,6,5,10,10,32
FBQOSCFG 4,D,5,6,5,10,10,32
FBQOSCFG 5,D,5,6,5,10,10,32
FBQOSCFG 6,D,5,6,5,10,10,32
FBQOSCFG 7,D,5,6,5,10,10,32
FBQOSCFG 8,D,5,6,5,10,10,32
FBQOSCFG 9,D,5,6,5,10,10,32
FBQOSCFG 10,D,5,6,5,10,10,32
```

Item not Configured

Quality of Service settings
(these are default settings)

Caller ID (not configured;
one line for each remote
unit)

Remote Office 9150 unit

This section shows the configuration settings for the Remote Office 9150 unit. You can obtain a similar configuration printout by performing a configuration download while connected to the Remote Office 9150 unit.

Note: Configuration settings are separated by commas (,).

Configuration example

This configuration example uses the settings identified in the network diagram shown on page 361.

```

IPCFCFG 10.1.1.2,255.255.0.0,10.1.1.10
APPMODCFG 0,SPARE,TSIDSP
APPMODCFG 1,E,G729,G729
APPMODCFG 2,NC,NC
APPMODCFG 3,NC,NC
APPMODCFG 4,1,1,E,1,1,5556987,60655569870101,E,1,1,
5556988,60655569880101
APPMODCFG 5,NC,NC
APPMODCFG 6,NC,NC
APPMODCFG 7,NC,NC
SYSCFG 2, Remote site 1
ROUCFG 13:00,0,JAN-13-2000,911,#222,#333,#345,#456,E
ACCFG N

```

9150 unit's IP interface information:

- IP address
- Subnet mask
- IP gateway

On-board DSP module (module 0) and installed DSP application module (module 1)

ISDN BRI module configuration

- module number
- PSTN number for each B-channel
- SPID for each B-channel

Unit ID and node name

System configuration:

- Emergency service number
- System date and time
- SPRE codes

```
RLCDETCFG 1,3,0987654321,1234567890,E,10.2.1.1,E,6135551234,E,D
```

Host PBX connection information:

- RLC's unit ID
- security information (inbound and outbound security IDs)
- RLC's IP address
- RLC PSTN number

```
ROUDEVCFG 0,2,0,E,E,E,Bryan Dion,8734,04
ROUDEVCFG 1,2,1,E,E,E,Marc Horman,8707,04
ROUDEVCFG 2,2,2,E,E,E,Brad McAllister,8708,04
ROUDEVCFG 3,2,3,E,E,E,Andrew Wong,8760,04
ROUDEVCFG 4,2,4,E,E,E,Corey Smith,8709,04
ROUDEVCFG 5,2,5,E,E,E,Tracey Black,8743,04
ROUDEVCFG 6,0,E,E,E,John Brown,8611,04
```

Port (station) configuration:

- Port number
- Local and remote capability
- CPND
- DN
- Restricted digits

```
ROUDEVCFG 7,1,0
ROUDEVCFG 8,1,0
ROUDEVCFG 9,1,0
ROUDEVCFG 10,1,0
ROUDEVCFG 11,1,0
ROUDEVCFG 12,1,0
ROUDEVCFG 13,1,0
ROUDEVCFG 14,1,0
ROUDEVCFG 15,1,0
ROUDEVCFG 16,1,0
ROUDEVCFG 17,1,0
ROUDEVCFG 18,1,0
ROUDEVCFG 19,1,0
ROUDEVCFG 20,1,0
ROUDEVCFG 21,1,0
ROUDEVCFG 22,1,0
ROUDEVCFG 23,1,0
ROUDEVCFG 24,1,0
ROUDEVCFG 25,1,0
ROUDEVCFG 26,1,0
ROUDEVCFG 27,1,0
ROUDEVCFG 28,1,0
ROUDEVCFG 29,1,0
ROUDEVCFG 30,1,0
ROUDEVCFG 31,1,0
ROUDEVCFG 32,2,31,E,E,E,FAX,8664,900
```

Unconfigured ports

Note: The default capability is Remote.

Fax port configuration:

- Port number
- Local and remote capability
- CPND
- DN
- Restricted digits

```

FKEYCFG 0,2 TRN 12345678,3 CFW 4000,8 LC1 ,9 LC2 ,NC
FKEYCFG 1,2 TRN 12345678,3 CFW 4000,8 LC1 ,9 LC2 ,NC
FKEYCFG 2,2 TRN 12345678,3 CFW 4000,8 LC1 ,9 LC2 ,NC
FKEYCFG 3,2 TRN 12345678,3 CFW 4000,8 LC1 ,9 LC2 ,NC
FKEYCFG 4,2 TRN 12345678,3 CFW 4000,8 LC1 ,9 LC2 ,NC
FKEYCFG 5,2 TRN 12345678,3 CFW 4000,8 LC1 ,9 LC2 ,NC
FKEYCFG 6,8 LC1 ,9 LC2 ,NC

```

```

FKEYCFG 7,NC
FKEYCFG 8,NC
FKEYCFG 9,NC
FKEYCFG 10,NC
FKEYCFG 11,NC
FKEYCFG 12,NC
FKEYCFG 13,NC
FKEYCFG 14,NC
FKEYCFG 15,NC
FKEYCFG 16,NC
FKEYCFG 17,NC
FKEYCFG 18,NC
FKEYCFG 19,NC
FKEYCFG 20,NC
FKEYCFG 21,NC
FKEYCFG 22,NC
FKEYCFG 23,NC
FKEYCFG 24,NC
FKEYCFG 25,NC
FKEYCFG 26,NC
FKEYCFG 27,NC
FKEYCFG 28,NC
FKEYCFG 29,NC
FKEYCFG 30,NC
FKEYCFG 31,NC
FKEYCFG 32,NC

```

Local station feature keys configuration:

- Port number
- Feature key number
- Feature name
- DN (if applicable)
- locations of local call appearance keys 1 and 2

Trunk group configuration:

- Trunk group number
- Trunk access code
- B-channels (ISDN module and B-channel number)
- DNS to alert

```

TRKGRPCFG 1,E,#61,4.0.0 4.0.1,8739
TRKGRPCFG 2,D,#62,1.0.0 1.0.1 2.0.0 2.0.1,4002
TRKGRPCFG 3,D,#63,1.0.0 1.0.1 2.0.0 2.0.1,4004
TRKGRPCFG 4,D,#64,1.0.0 1.0.1 2.0.0 2.0.1,4006
TRKGRPCFG 5,D,#65,1.0.0 1.0.1 2.0.0 2.0.1,4008
TRKGRPCFG 6,D,#66,1.0.0 1.0.1 2.0.0 2.0.1,4010
TRKGRPCFG 7,D,#67,1.0.0 1.0.1 2.0.0 2.0.1,4012
TRKGRPCFG 8,D,#68,1.0.0 1.0.1 2.0.0 2.0.1,4014

```

Item not Configured

← Caller ID (not configured)

Appendix C

Connection pin-out tables

In this appendix

TELCO 1 connector pin-out table	374
TELCO 2 connector pin-out table	376
Ethernet connector pin-out table	378
Admin (serial) connector pin-out table	379
Power connector pin-out table	380

TELCO 1 connector pin-out table

Note: The colors shown in this table represent standard telephone cable pin-outs.

Port or module	Pin #	Signal	Color	Pin #	Signal	Color
Digital port 0	1	DP 0 RING	BL-W	26	DP 0 TIP	W-BL
Digital port 1	2	DP 1 RING	OR-W	27	DP 1 TIP	W-OR
Digital port 2	3	DP 2 RING	GR-W	28	DP 2 TIP	W-GR
Digital port 3	4	DP 3 RING	BR-W	29	DP 3 TIP	W-BR
Digital port 4	5	DP 4 RING	SL-W	30	DP 4 TIP	W-SL
Digital port 5	6	DP 5 RING	BL-R	31	DP 5 TIP	R-BL
Digital port 6	7	DP 6 RING	OR-R	32	DP 6 TIP	R-OR
Digital port 7	8	DP 7 RING	GR-R	33	DP 7 TIP	R-GR
Digital port 8	9	DP 8 RING	BR-R	34	DP 8 TIP	R-BR
Digital port 9	10	DP 9 RING	SL-R	35	DP 9 TIP	R-SL
Digital port 10	11	DP 10 RING	BL-B	36	DP 10 TIP	B-BL
Digital port 11	12	DP 11 RING	OR-B	37	DP 11 TIP	B-OR
Digital port 12	13	DP 12 RING	GR-B	38	DP 12 TIP	B-GR
Digital port 13	14	DP 13 RING	BR-B	39	DP 13 TIP	B-BR
Digital port 14	15	DP 14 RING	SL-B	40	DP 14 TIP	B-SL
Digital port 15	16	DP 15 RING	BL-Y	41	DP 15 TIP	Y-BL
Leave open for UL spacing requirements	17	Open	OR-Y	42	Open	Y-OR
Module 4 (ISDN BRI—ST only)	18	MOD 3 Tip 0+	GR-Y	43	Module 3 Tip 0-	Y-GR

Port or module	Pin #	Signal	Color	Pin #	Signal	Color
Module 4 (ISDN BRI—U or ST)	19	MOD 3 Ring 0+	BR-Y	44	Module 3 RING 0-	Y-BR
Module 5 (ISDN BRI—ST only)	20	MOD 4 Tip 0+	SL-Y	45	Module 4 Tip 0-	Y-SL
Module 5 (ISDN BRI—U or ST)	21	MOD 4 Ring 0+	BL-V	46	Module 4 RING 0-	V-BL
Module 5 (for future use)	22	MOD 4 Tip 1+	OR-V	47	Module 4 TIP 1-	V-OR
Module 5 (for future use)	23	MOD 4 Ring 1+	GR-V	48	Module 4 RING 1-	V-GR
Leave open for UL spacing requirements	24	Open	BR-V	49	UK Ring	V-BR
Analog port	25	AP TIP	SL-V	50	AP RING	V-SL

TELCO 2 connector pin-out table

Note: The colors shown in this table represent standard telephone cable pin-outs.

Port or module	Pin #	Signal	Color	Pin #	Signal	Color
Digital port 16	1	DP 16 RING	BL-W	26	DP 16 TIP	W-BL
Digital port 17	2	DP 17 RING	OR-W	27	DP 17 TIP	W-OR
Digital port 18	3	DP 18 RING	GR-W	28	DP 18 TIP	W-GR
Digital port 19	4	DP 19 RING	BR-W	29	DP 19 TIP	W-BR
Digital port 20	5	DP 20 RING	SL-W	30	DP 20 TIP	W-SL
Digital port 21	6	DP 21 RING	BL-R	31	DP 21 TIP	R-BL
Digital port 22	7	DP 22 RING	OR-R	32	DP 22 TIP	R-OR
Digital port 23	8	DP 23 RING	GR-R	33	DP 23 TIP	R-GR
Digital port 24	9	DP 24 RING	BR-R	34	DP 24 TIP	R-BR
Digital port 25	10	DP 25 RING	SL-R	35	DP 25 TIP	R-SL
Digital port 26	11	DP 26 RING	BL-B	36	DP 26 TIP	B-BL
Digital port 27	12	DP 27 RING	OR-B	37	DP 27 TIP	B-OR
Digital port 28	13	DP 28 RING	GR-B	38	DP 28 TIP	B-GR
Digital port 29	14	DP 29 RING	BR-B	39	DP 29 TIP	B-BR
Digital port 30	15	DP 30 RING	SL-B	40	DP 30 TIP	B-SL
Digital port 31	16	DP 31 RING	BL-Y	41	DP 31 TIP	Y-BL
Leave open for UL spacing requirements	17	Open	OR-Y	42	Open	Y-OR
Module 6 (ISDN BRI—ST only)	18	MOD 5 Tip 0+	GR-Y	43	Module 5 Tip 0-	Y-GR

Port or module	Pin #	Signal	Color	Pin #	Signal	Color
Module 6 (ISDN BRI—U or ST)	19	MOD 5 Ring 0+	BR-Y	44	Module 5 Ring 0-	Y-BR
Module 7 (ISDN BRI—ST only)	20	MOD 6 Tip 0+	SL-Y	45	Module 6 Tip 0-	Y-SL
Module 7 (ISDN BRI—U or ST)	21	MOD 6 Ring 0+	BL-V	46	Module 6 Ring 0-	V-BL
Module 7 (for future use)	22	MOD 6 Tip 1+	OR-V	47	Module 6 Tip 1-	V-OR
Module 7 (for future use)	23	MOD 6 Ring 1+	GR-V	48	Module 6 Ring 1-	V-GR
Leave open for UL spacing requirements	24	Open	BR-V	49	Open	V-BR
Fault Relay Contact 1	25	FLT RLY 1	SL-V	50	FLT RLY 2	V-SL

Ethernet connector pin-out table

Pin number	Signal name	I/O	Description
1	TX+	O	Transmit Clock +
2	TXC	I	Transmit Clock Common (Ground)
3	TX-	O	Transmit Clock -
4	Chassis Ground	I	Shield
5	Chassis Ground	I	Shield
6	RXC	I	Receive Clock Common (Ground)
7	RX+	I	Receive Clock +
8	RX-	I	Receive Clock -

Admin (serial) connector pin-out table

Pin number	Signal name	I/O	Description
1			
2	MMI-RXD	I	MMI RS-232C Receive Data
3	MMI-TXD	O	MMI RS-232C Transmit Data
4			
5	Ground	I	Logic Ground
6			
7			
8			
9			

Power connector pin-out table

Pin number	Signal name	I/O	Current	Description
1	+5V	I	5.0 A	+5v
2	Ground	I		Logic Ground
3	+24V	I	1.5 A	+24v
4	-12V	I	0.1 A	+24v

Appendix D

Display log definitions

In this appendix

Display logs

382

Display logs

The display log functionality is significantly improved over prior releases of Remote Office 9150. This appendix lists the 9150 system's display log error and status messages.

Statistic	Definition
LOG NUMBER	0
DESCRIPTION	This is a description of the log that is being generated.
SEVERITY	NORMAL, WARNING, MINOR, MAJOR, CRITICAL (Assigns one of these levels to the Log.)
TASK	This is the task that originates the trap. This can be the full name or an abbreviation. (For development use only.)
PRODUCT	RLC, 9150, 911x (Lists all products that can generate this log.)
CANCELLATION	This is a cross-reference to another log number that is the complement of the current log (for example, QOS Transition/Recovery, Link Up/Down.) This should be a LOG NUMBER and send Log IDType.
ACTION TO BE TAKEN:	If the Severity is higher than NORMAL, this should contain information that would help the end user correct the problem, if possible (for example, a Configuration Change), or give them information about where the user should go for help.
PARAMETERS	1) description of parameter 1 2) description of parameter 2 . . . N) description of parameter N
DISPLAYED TEXT	Formatting String

Statistic	Definition
LOG NUMBER	1
DESCRIPTION	This log indicates that system started.
SEVERITY	NORMAL
TASK	MMI
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	None
DISPLAYED TEXT	System started

LOG NUMBER	2
DESCRIPTION	This logs indicates that there was a failure in allocation of the TCM block
SEVERITY	CRITICAL
TASK	None
PRODUCT	9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	TCM buffer is exhausted. If the problem persists reboot the system and report back to vendor.
PARAMETERS	None
DISPLAYED TEXT	Out of TCM buffer

Statistic	Definition
LOG NUMBER	3
DESCRIPTION	This logs indicates that there was a failure in allocation of memory of size 'n'.
SEVERITY	MAJOR
TASK	None
PRODUCT	9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	Memory buffers exhausted. If the problem persists reboot the system.
PARAMETERS	Size of memory block that the system failed to allocate.
DISPLAYED TEXT	Couldn't allocate memory of size P1.

LOG NUMBER	4
DESCRIPTION	This logs indicates that there was a failure in sending a message to a Remote Office unit.
SEVERITY	MAJOR
TASK	None
PRODUCT	9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	1) The destination host is unreachable check its status. 2) Check the configuration.
PARAMETERS	Unit ID of remote board for which message was intended.
DISPLAYED TEXT	Couldn't send message to unit ID: P1

Statistic	Definition
LOG NUMBER	5
DESCRIPTION	This log indicates that the QoS of the IP network degraded and the system transitioned to the PSTN.
SEVERITY	NORMAL
TASK	QoS Transitioning
PRODUCT	RLC, 9150, 911x
CANCELLATION	Log number 2 - FB_RECOVERY_LOG_ID
ACTION TO BE TAKEN	Investigate why the IP network was determined to be below VoIP quality. Review the Engineering Guidelines.
PARAMETERS	Unit ID of the Remote Office unit for which the IP QoS has degraded.
DISPLAYED TEXT	Transition to remote site: P1

LOG NUMBER	6
DESCRIPTION	This log indicates that the QoS of the IP network recovered and the system transitioned to the IP Network.
SEVERITY	NORMAL
TASK	Fallback
PRODUCT	RLC, 9150, 911x
CANCELLATION	Log number 1 - FB_FALLBACK_LOG_ID
ACTION TO BE TAKEN	Investigate why the IP network was determined to be below VoIP quality. Review the Engineering Guidelines.
PARAMETERS	Unit ID of the Remote Office unit for which the IP QOS has recovered.
DISPLAYED TEXT	Recovery to remote site: P1

Statistic	Definition
LOG NUMBER	7
DESCRIPTION	This log indicates that a user logged onto the system
SEVERITY	NORMAL
TASK	Session Control
PRODUCT	RLC, 9150, 911x
CANCELLATION	Log number 8
ACTION TO BE TAKEN	None
PARAMETERS	Connection (serial or Telnet) through which user logged onto system.
DISPLAYED TEXT	User logged on: P1
LOG NUMBER	8
DESCRIPTION	This log indicates that a user logged off from the system.
SEVERITY	NORMAL
TASK	Session Control
PRODUCT	RLC, 9150, 911x
CANCELLATION	Log number 7
ACTION TO BE TAKEN	None
PARAMETERS	Logoff type – normal or terminated.
DISPLAYED TEXT	User logged off: P1

Statistic	Definition
LOG NUMBER	9
DESCRIPTION	This log indicates that logon to the system failed.
SEVERITY	WARNING
TASK	Session Control
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	Reason – wrong user name, password, device busy etc.
DISPLAYED TEXT	User login failed: P1
LOG NUMBER	10
DESCRIPTION	This log indicates a debug Session Terminated. A debug session that was inactive for more than 15 minutes was automatically logged off from the system.
SEVERITY	NORMAL
TASK	Session Control
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	Reason for termination
DISPLAYED TEXT	Debug session terminated: P1

Statistic	Definition
LOG NUMBER	11
DESCRIPTION	This log indicates that database reading from flash at Power on failed. This can be caused by corrupted flash. As a result, the system starts with the default configuration.
SEVERITY	CRITICAL
TASK	MMI
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	1) Reconfigure the system and then save it to Flash. Note: When you save configuration changes to Flash, the system suspends new call processing for approximately 30 seconds. 2) Restart the system and log into the system and check the configured parameters. If the problem persists contact your vendor.
PARAMETERS	Reason reading from Flash failed.
DISPLAYED TEXT	Database reading from Flash failed - P1
LOG NUMBER	12
DESCRIPTION	This log indicates that user tried saving a new configuration to Flash.
SEVERITY	NORMAL
TASK	MMI
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	Status of Save to Flash – success or failure
DISPLAYED TEXT	Database save to Flash: P1

Statistic	Definition
LOG NUMBER	13
DESCRIPTION	This log indicates that a user defaulted the configuration of the board using the Set default configuration command.
SEVERITY	NORMAL
TASK	MMI
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	None
DISPLAYED TEXT	Database defaulted
LOG NUMBER	14
DESCRIPTION	This log indicates that User tried a configuration upload.
SEVERITY	NORMAL
TASK	MMI
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	1) Status - success or failure 2) Name of configuration file 3) IP address of source of configuration file
DISPLAYED TEXT	Database upload: P1 (P2 from P3)

Statistic	Definition
LOG NUMBER	15
DESCRIPTION	This log indicates that a n application module is enabled and not plugged in. This can happen when the user configures a module and then removes it from the system.
SEVERITY	MAJOR
TASK	MMI
PRODUCT	RLC, 9150
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	1) Module type 2) Mismatch details
DISPLAYED TEXT	Application module configuration mismatch: P1 P2.

Statistic	Definition
LOG NUMBER	16
DESCRIPTION	This log indicates that there is a DN clash. This can happen in the following cases: ■ Same DNs configured for multiple ports. ■ Same access codes configured for trunk groups. ■ Same SPRE code is configured for different functions. ■ A longer DN number exists.
SEVERITY	MAJOR
TASK	MMI
PRODUCT	9150
CANCELLATION	None
ACTION TO BE TAKEN	Check for duplication of configuration (Use "Get DN List" to see the data) and correct it.
PARAMETERS	1) Type of Data 2) First clashing port number
DISPLAYED TEXT	DN clash: P1 P2 P3

Statistic	Definition
LOG NUMBER	17
DESCRIPTION	This log indicates that the User tried to upload software. This could be application software or ISDN module software. After an application software upload, the system is normally restarted. Therefore, it is possible that this log was lost.
SEVERITY	NORMAL
TASK	MMI
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	1) Status - success or failure 2) Module type - application or ISDN 3) File name 4) Source of file (for example, IP address)
DISPLAYED TEXT	Software upload: P1 (P2, P3 from P4)

LOG NUMBER	18
DESCRIPTION	This log indicates that a user tried a cross connection to PBX over RS232 Port using the Xconnect command.
SEVERITY	NORMAL
TASK	MMI
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	Status of cross-connect attempt - success or failure
DISPLAYED TEXT	User cross connect to PBX: P1

Statistic	Definition
LOG NUMBER	19
DESCRIPTION	This log indicates that a user tried a Remote connection to another system using the Telnet command.
SEVERITY	NORMAL
TASK	MMI
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	1) Status of Telnet attempt - success or failure 2) Destination (for example, IP address)
DISPLAYED TEXT	User remote connection: P1 P2

LOG NUMBER	20
DESCRIPTION	This log indicates the power on initialization of the ports completed.
SEVERITY	NORMAL
TASK	CallProcessing
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	None
DISPLAYED TEXT	Power-on initialization of ports completed.

Statistic	Definition
LOG NUMBER	21
DESCRIPTION	This log indicates that the remote site re-initialized upon Remote Office unit configuration change.
SEVERITY	NORMAL
TASK	CallProcessing
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	Unit ID of the Remote Office unit re-initialized
DISPLAYED TEXT	Remote site: P1 is re-initialized

LOG NUMBER	22
DESCRIPTION	This log signals that the link to the specified Remote Office unit went down.
SEVERITY	MAJOR
TASK	CallProcessing
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	Unit ID of the Remote Office unit to which the link went down
DISPLAYED TEXT	Link down for remote site: P1

Statistic	Definition
LOG NUMBER	23
DESCRIPTION	This log indicates that a Remote Office unit registered.
SEVERITY	NORMAL
TASK	CallProcessing
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	Unit ID of the Remote Office unit that registered.
DISPLAYED TEXT	Remote site: P1 is registered.
LOG NUMBER	24
DESCRIPTION	This log signals a port registration clash for a dedicated port.
SEVERITY	WARNING
TASK	CallProcessing
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	Possible mis-configuration on remote. Check the configurations
PARAMETERS	1) port number of first clashing remote port 2) unit ID of the remote on which first clashing port resides 3) number of dedicated RLC port for which there is a clash 4) port number of second clashing remote port 5) unit ID of the remote on which the second clashing port resides
DISPLAYED TEXT	Registration clash for port P1 on remote site: P2 with port P3 on the RLC. Dedicated port P3 is already registered with port P4 of the remote site: P5

Statistic	Definition
LOG NUMBER	25
DESCRIPTION	This log indicates that a remote port registered with a multiuser/dynamic RLC port.
SEVERITY	NORMAL
TASK	CallProcessing
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	1) Port number of remote port registered on multiuser/dynamic port 2) Unit ID of remote on which remote port resides 3) Port number of multiuser/dynamic port on RLC
DISPLAYED TEXT	Port P1 on remote site: P2 is registered with multiuser /dynamic pool port P3.

Statistic	Definition
LOG NUMBER	26
DESCRIPTION	This log indicates a port registration clash for a Multiuser port.
SEVERITY	MAJOR
TASK	CallProcessing
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	1) number of remote port for which there is a registration clash 2) unit ID of the Remote Office unit on which port resides 3) port number of multiuser port on RLC 4) port number of currently registered remote port 5) unit ID of the Remote Office unit on which currently registered port resides
DISPLAYED TEXT	Registration clash for port P1 on remote site: P2 with multiuser port P3. Multiuser port P3 is already registered with port P4 on remote site P5

Statistic	Definition
LOG NUMBER	27
DESCRIPTION	This log indicates that a port registration failed for a dynamic pool port. All ports in this dynamic pool are registered and no port is available for use.
SEVERITY	MAJOR
TASK	CallProcessing
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	1) Port number on remote for which there is a registration failure. 2) Unit ID of the Remote Office unit on which port resides
DISPLAYED TEXT	Registration failed for dynamic pool port P1 on remote site: P2

Statistic	Definition
LOG NUMBER	28
DESCRIPTION	This logs indicates that there was a failure in allocation of a new call register.
SEVERITY	CRITICAL
TASK	Device Control, Call Processing
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	The system memory allocation has failed and might have been exhausted. If the problem persists reboot the system.
PARAMETERS	port number
DISPLAYED TEXT	Call register allocation failed in local calling on Port P1.

LOG NUMBER	29
DESCRIPTION	This log indicates that there were insufficient DSP channels when a voice call was attempted.
SEVERITY	MINOR
TASK	Device Control/Call Processing
PRODUCT	9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	1) All the DSP channels on the system are in use. Wait for calls to be dropped. 2) To avoid blocking, either distribute calls onto additional RLCs and 9150s, or add DSP modules to existing equipment, provided there is space available for additional modules. Otherwise action # 1 applies.
PARAMETERS	port number
DISPLAYED TEXT	DSP resource allocation failed on Port P1

Statistic	Definition
LOG NUMBER	30
DESCRIPTION	This log indicates that allocation of a local trunk for a local call failed. The possible reasons for failure are: 1) All the trunks are in use. 2) There are no Local or Local/Remote trunks configured. 3) The BRI link may be down or the BRI module might not be plugged in completely.
SEVERITY	MINOR
TASK	Device Control
PRODUCT	9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	1) Confirm that the BRI modules are plugged in properly and the BRI link is UP. 2) Confirm that the BRI configuration is correct.
PARAMETERS	port number
DISPLAYED TEXT	Local trunk allocation failed on port P1.

Statistic	Definition
LOG NUMBER	31
DESCRIPTION	This log indicates that a local call failed because the dialed DN didn't exist.
SEVERITY	WARNING
TASK	Device Control
PRODUCT	9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	Verify the dialed digits with the configuration numbers.
PARAMETERS	Dialed digits.
DISPLAYED TEXT	Unassigned number P1

LOG NUMBER	32
DESCRIPTION	This log indicates that a local call failed because the sequence of Dialed digits is not allowed on the set that is attempting to place the call.
SEVERITY	WARNING
TASK	Device Control
PRODUCT	9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	Verify that the dialed digits don't match the disabled outbound digits.
PARAMETERS	dialed digits
DISPLAYED TEXT	Disabled outbound digits blocked P1

Statistic	Definition
LOG NUMBER	33
DESCRIPTION	This log indicates that the DSP cross connect failed, which might have resulted in no voice path being established.
SEVERITY	CRITICAL
TASK	Device Control
PRODUCT	9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	Contact the vendor if the problem persists
PARAMETERS	port number
DISPLAYED TEXT	DSP cross connect failed on port P1

LOG NUMBER	34
DESCRIPTION	This log indicates a change in the system Mode
SEVERITY	NORMAL
TASK	Device Control, Call Processing
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	Status: online/offline
DISPLAYED TEXT	Changing system mode to: P1

Statistic	Definition
LOG NUMBER	35
DESCRIPTION	This log indicates that there was a failure in registering to a remote RLC. This would indicate that the Host is unreachable through both the IP and the PSTN.
SEVERITY	MAJOR
TASK	Device Control
PRODUCT	9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	1) Check for the IP/PSTN connectivity. 2) Check for the remote Host status. 3) Check the correctness of configuration. Units should be enabled.
PARAMETERS	Unit ID of remote site to which registration failed.
DISPLAYED TEXT	Failed to register to remote site: P1

Statistic	Definition
LOG NUMBER	36
DESCRIPTION	This log indicates the success or failure of a Remote Office 9150 unit port's attempt to register with a Multiuser/Dynamic port on a RLC.
SEVERITY	NORMAL
TASK	Device Control
PRODUCT	RLC, 9150
CANCELLATION	None
ACTION TO BE TAKEN	1) Determine if the port was in use. 2) Configure the port as a Multiuser/Dynamic port. 3) The host RLC is unreachable.
PARAMETERS	1) 9150 unit's port number attempting to register with the multiuser/dynamic port on the RLC 3) registered or unregistered status of 9150 unit's port 4) port number of multiuser/dynamic port on RLC
DISPLAYED TEXT	ROU port P1, P2 to RLC port P3

Statistic	Definition
LOG NUMBER	37
DESCRIPTION	This log indicates that an attempt to connect to a Remote Office unit on the specified medium failed. 1) If the same message is displayed with both IP and PSTN, in succession, the specified remote cannot be reached. 2) If only one message displays with a specific medium while connections on other medium are fine, it indicates a possible attempt to connect on the medium due to: a) Priority of the call that requires only that medium. Voice call would have failed. Check for log number 55 b) IP QoS state and priority level required a first attempt on the specified medium. A voice call would have succeeded on the other medium, though it cannot be guaranteed. c) Attempt was made on receiving a QoS status message.
SEVERITY	MAJOR
TASK	Network Manager
PRODUCT	RLC, 9150, 911 x
CANCELLATION	None
ACTION TO BE TAKEN	Verify the following: 1) correctness of configurations 2) whether the network connections are proper 3) status of the remote board
PARAMETERS	1) Remote Office unit ID 2) medium on which the attempt failed
DISPLAYED TEXT	Not able to connect to remote site: P1 on P2 medium

Statistic	Definition
LOG NUMBER	38
DESCRIPTION	This log indicates that an attempt to bring up an additional trunk failed due to the lack of an unoccupied, configured trunk. This could cause the failure of a voice call depending on the media allowed to communicate to that remote, the priority of the call, and the Extra Bandwidth configured. However, verify the presence of log number 55 on the RLC to see if a voice call did not succeed. Look for the presence of log number 37 on the RLC. It indicates that an attempt was made to connect the voice call on that medium, but that the medium was not reachable.
SEVERITY	MINOR
TASK	Network Manager
PRODUCT	RLC, 9150
CANCELLATION	None
ACTION TO BE TAKEN	Verify for the specified log numbers and note them. If this happens frequently, new trunks may have to be added.
PARAMETERS	Remote Office unit ID
DISPLAYED TEXT	No free additional trunk available to remote site: P1

Statistic	Definition
LOG NUMBER	39
DESCRIPTION	This log indicates that there an attempt was made to get an additional trunk on the PSTN. This message should have a corresponding message with same number on the Remote Office 9150 unit board. This might cause a voice call to fail, depending on the media allowed to communicate with that remote device and the priority of the call. However, check for the presence of log number 55 on the RLC to see if a voice call did not succeed. Look for the presence of log number 37 on the RLC. It indicates that an attempt was made to connect the voice call on that medium, but that the medium was not reachable.
SEVERITY	MINOR
TASK	Network Manager
PRODUCT	RLC, 9150
CANCELLATION	None
ACTION TO BE TAKEN	1) Ensure the PSTN numbers shown in Trunk Configuration are correct on both the RLC and Remote Office 9150 unit. 2) Ensure the trunk route to that Remote Office unit is not busy.
PARAMETERS	1) Remote Office unit ID 2) PSTN number attempted 3) A flag to indicate whether attempt is made by remote board or local board. 1 - indicates attempt made by local board 2 - indicates attempt made by remote board
DISPLAYED TEXT	Attempted bring-up additional trunk failed. remote P1, PSTN number P2, flag P3

Statistic	Definition
LOG NUMBER	40
DESCRIPTION	This log indicates that an attempt to transition to the PSTN failed. Appearance of this message does not cause a voice call to drop. However, if RLC Log numbers 42 or 56 appear, the system can drop voice calls and not be able to connect to the Remote Office unit temporarily.
SEVERITY	WARNING
TASK	Network Manager
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	a) Look for correctness of primary PSTN number. If PSTN is disabled, ignore this message b) Trunk route might be busy to that remote. c) If the specified logs also appear, IP network could be down
PARAMETERS	Remote Office unit ID
DISPLAYED TEXT	Transition did not happen to remote site: P1

Statistic	Definition
LOG NUMBER	41
DESCRIPTION	This log indicates the failure of the system to connect to the specified remote on the IP network due to a network problem other than unacceptable QoS.
SEVERITY	WARNING
TASK	Network Manager
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	1) Check for problems on IP network. 2) Wait for more attempts because connections can take more time depending on nature of the network.
PARAMETERS	Remote Office unit ID
DISPLAYED TEXT	Attempt to recover to IP network failed to remote site: P1

Statistic	Definition
LOG NUMBER	42
DESCRIPTION	This log indicates that the IP network failed abruptly while there were connections routed over IP, dropping active voice calls. To check for dropped voice calls, look for log number 56.
SEVERITY	MAJOR
TASK	Network Manager
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	Check if the IP connection is intact or if there is another problem on the IP network.
PARAMETERS	Remote Office unit ID
DISPLAYED TEXT	Abnormal failure of IP network. remote site: P1

LOG NUMBER	43
DESCRIPTION	This log indicates the failure of a non-primary trunk. This might lead to dropping of voice calls to compensate the BW loss in the absence of an IP connection to the Remote Office unit. Look for log number 56 to see if any calls were dropped.
SEVERITY	MAJOR
TASK	Network Manager
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	1) Verify that the PSTN connections are OK. 2) If this displays on the RLC, look for log number 46 on the 9150 unit. If this ID is there, it is a genuine closure. 3) Link might have failed somewhere in the PSTN.
PARAMETERS	Remote Office unit ID
DISPLAYED TEXT	Abnormal failure of one of the trunks. remote site: P1

Statistic	Definition
LOG NUMBER	44
DESCRIPTION	This log indicates an abnormal failure of the primary signaling link. This leads to the dropping of all active connections to the Remote Office unit.
SEVERITY	CRITICAL
TASK	Network Manager
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	1) Check IP and trunk connections. (physical connections) 2) If this displays on the RLC, look for log number 45 on the 9150 unit. If this log is there, it is a genuine closure. 3) Link might have failed some where in the Public network.
PARAMETERS	Remote Office unit ID to which communication is lost
DISPLAYED TEXT	Abnormal failure of primary signaling to remote site: P1

Statistic	Definition
LOG NUMBER	45
DESCRIPTION	This log indicates that the primary signaling was dropped due to a request for a 911 (emergency) call, resulting in a temporary loss of communication with RLC.
SEVERITY	WARNING
TASK	Network Manager
PRODUCT	9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	This indicates that there are not enough trunks and the primary trunk had to be used for a 911 (emergency) call. Check if number of trunks can be increased (9150 only).
PARAMETERS	None
DISPLAYED TEXT	Primary trunk dropped to place 911 call

LOG NUMBER	46
DESCRIPTION	This log indicates that the system dropped one of the additional trunks to place a 911 (emergency) call as there were no available trunks.
SEVERITY	WARNING
TASK	Network Manager
PRODUCT	9150
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	None
DISPLAYED TEXT	Closing an additional trunk to place 911 call

Statistic	Definition
LOG NUMBER	47
DESCRIPTION	This log indicates that inactivity timer creation failed. This could lead to the primary signaling channel not closing to the remote. If the IP QoS is BAD, the PSTN trunk stays on. Otherwise, IP stay on.
SEVERITY	WARNING
TASK	Network Manager
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	To overcome this situation, make sure no one is using the Remote Office unit phones, and then go to offline mode and come back to on-line. Normal operation is restored. Use online/offline spree codes on the 9150, 911x unit.
PARAMETERS	Remote Office unit ID
DISPLAYED TEXT	Timer creation failed. Signal will not be closed to remote site: P1

Statistic	Definition
LOG NUMBER	48
DESCRIPTION	This log indicates the failure of a connection because of incorrect security information due to one of the following situations: 1) A Valid remote tried to connect with inappropriate Security data. 2) The Remote Office unit rejected a connection initiated by the local unit. 3) There is a security issue with bringing up an additional trunk.
SEVERITY	WARNING
TASK	Network Manager
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	1) Check that the security levels and security IDs are correct in configuration. 2) Security issue for additional trunks comes up if security level is CLID security and configuration is improper. 3) This may be an indication of an unauthorized Remote Office unit attempting to connect.
PARAMETERS	1) Remote Office unit ID 2) media 3) connection type: primary/additional
DISPLAYED TEXT	Security failure to remote site: P1 on medium P2.

Statistic	Definition
LOG NUMBER	49
DESCRIPTION	This log indicates that an unknown remote tried to connect and the attempt failed.
SEVERITY	WARNING
TASK	Network Manager
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	1) Confirm that the configuration of the unit IDs are OK between the units. 2) This may be an indication of an unauthorized Remote Office unit attempting to connect.
PARAMETERS	Unit ID of the Remote Office unit
DISPLAYED TEXT	Message from invalid remote site: P1

Statistic	Definition
LOG NUMBER	50
DESCRIPTION	This log indicates that a connection came in on an unconfigured port and was rejected by the system. (PSTN connections)
SEVERITY	WARNING
TASK	Network Manager
PRODUCT	RLC, 9150
CANCELLATION	None
ACTION TO BE TAKEN	1) Check for proper port configurations on the RLC and 9150 unit. 2) Check if a local call came in on a remote-only BRI port. Ensure that non-remote only BRI trunk numbers only are given to outsiders to call 9150's local sets. 3) Unauthorized unit may be trying to connect. Verify!
PARAMETERS	PSTN number from which the call originates
DISPLAYED TEXT	Incoming connection rejected. Address P1

Statistic	Definition
LOG NUMBER	51
DESCRIPTION	This log indicates that an incoming connection from the specified Remote Office unit failed because the specified medium is not allowed to connect to that Remote Office unit.
SEVERITY	WARNING
TASK	Network Manager
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	1) Check the correctness of configurations. 2) Verify that unit trying to connect has needed authorization.
PARAMETERS	1) Unit ID of the Remote Office unit 2) The medium to which it attempted to connect
DISPLAYED TEXT	Signaling clash to remote site: P1 [on medium: P2]
LOG NUMBER	52
DESCRIPTION	This log indicates that no activity was found on the signaling link and all remote service phones were idle.
SEVERITY	NORMAL
TASK	Network Manager
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	None. This is part of normal system operation.
PARAMETERS	Remote Office unit ID
DISPLAYED TEXT	Signaling closed to remote site: P1 due to no activity

Statistic	Definition
LOG NUMBER	53
DESCRIPTION	This log indicates that the Remote Office unit went Offline. No communication is possible until the unit goes Online again or Online time occurs. In Offline mode, all connections, including permanent trunks, if any, are closed.
SEVERITY	NORMAL
TASK	Network Manager
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	Remote Office unit ID going offline
DISPLAYED TEXT	Close signal as unit goes offline. remote site: P1

Statistic	Definition
LOG NUMBER	54
DESCRIPTION	This log indicates an attempt to reach an invalid remote.
SEVERITY	WARNING
TASK	Network Manager
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	1) Check for proper configuration 2) Check for updates completed while system was active. 3) If the message is consistent, even after proper configuration, report to vendor.
PARAMETERS	unit ID of Remote Office unit to which connection was attempted.
DISPLAYED TEXT	Connection attempted to invalid remote site: P1

Statistic	Definition
LOG NUMBER	55
DESCRIPTION	This log indicates the system was unable to place a voice call, which could be caused by the following conditions: 1) No connection to the remote. Attempts failed. 2) HIGH/NORMAL priority: No BW on trunk and IP not available. 3) PSTN only call: No BW available, trunk disabled, or trunk not reachable. 4) IP only call: IP not reachable or not enabled. 5) Some inconsistency within the system - Synchronization between RLC - 9150/911x.
SEVERITY	NORMAL
TASK	Network Manager
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	1) Verify correctness of configurations. 2) Verify physical connections on the medium as per information in 1), above. Note: If this happens consistently for all calls, and is not an obvious problem due to configuration or BW limitations, view the statistics and report the problem.
PARAMETERS	1) Remote Office unit ID 2) amount of bandwidth the system needs to place the additional call
DISPLAYED TEXT	Voice call did not succeed to remote site: P1 [BW required P2]

Statistic	Definition
LOG NUMBER	56
DESCRIPTION	This log indicates an abnormal failure of a call. Possible reasons include: 1) sudden link failure on the given medium 2) drop of remote trunks on the 9150/911x side for a 911 (emergency) call 3) sudden primary signaling failure
SEVERITY	MAJOR
TASK	Network Manager
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	Look for log numbers 42, 43, and 44 to ascertain the reason active calls were dropped.
PARAMETERS	1) bandwidth of the call 2) unit ID of remote to which call is connected 3) media on which the call was active at the time of failure
DISPLAYED TEXT	Call of P1 BW got dropped to remote site: P2, medium: P3

Statistic	Definition
LOG NUMBER	57
DESCRIPTION	This log indicates a failed attempt to switch a voice connection to the specified medium. This is an indication of a loss of one of the following: 1) signaling packets 2) synchronization between RLC - 9150, 911x
SEVERITY	MINOR
TASK	Network Manager
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	This should not happen in general. If it does, report the problem.
PARAMETERS	1) bandwidth of the call 2) medium from which the system attempted to switch the call 3) medium to which the system attempted to switch the call 4) Remote Office unit ID
DISPLAYED TEXT	Call of P1 BW did not switch from medium: P2 to medium: P3. remote site: P4

Statistic	Definition
LOG NUMBER	58
DESCRIPTION	This log indicates that there is no available trunk in the given trunk group to place a local trunk call.
SEVERITY	MINOR
TASK	Network Manager
PRODUCT	9150
CANCELLATION	None
ACTION TO BE TAKEN	If this happens consistently, think of reconfiguring B-channel allocations on 9150
PARAMETERS	Trunk Group Number
DISPLAYED TEXT	Local call did not succeed.

Statistic	Definition
LOG NUMBER	59
DESCRIPTION	This log indicates that a local call was dropped because of an abnormal link failure.
SEVERITY	MAJOR
TASK	Network Manager
PRODUCT	9150
CANCELLATION	None
ACTION TO BE TAKEN	■ Confirm that physical trunk connections are intact ■ Check for failure on the PSTN.
PARAMETERS	None
DISPLAYED TEXT	Local trunk call abnormally failed.

LOG NUMBER	60
DESCRIPTION	This message indicates that a local trunk call was dropped for an emergency (911) call because there were no free trunks.
SEVERITY	WARNING
TASK	Network Manager
PRODUCT	9150
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	None
DISPLAYED TEXT	Local call dropped for 911.

Statistic	Definition
LOG NUMBER	61
DESCRIPTION	This log indicates that the signaling link to a Remote Office unit was established on the specified medium.
SEVERITY	NORMAL
TASK	Network Manager
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	Nothing. This is part of normal system operation.
PARAMETERS	Remote Office unit ID
DISPLAYED TEXT	Signaling is UP to remote site: P1 on medium: P2.

LOG NUMBER	62
DESCRIPTION	This log indicates that the IDVR server has gone down. (This log is not generated in the 1.2.1 release.)
SEVERITY	MAJOR
TASK	Device Control, Call processing
PRODUCT	RLC, 9150, IDVR
CANCELLATION	None
ACTION TO BE TAKEN	1) Check for the IP connectivity to server. 2) Check for the IDVR server status.
PARAMETERS	IDVR server's IP address.
DISPLAYED TEXT	IDVR server status: P1

Statistic	Definition
LOG NUMBER	63
DESCRIPTION	This log indicates a PSTN connection to a peer unit failed. This could be caused by several possible problems, including: 1) A cabling issue at the Remote Office unit could keep that unit from being able to connect on the PSTN. 2) The data port on the RLC could be disabled. 3) For BRI connections between a 9150 and an RLC the PSTN path may not be a 64K clear channel (the required path). 4) Incorrect dial numbers could be keeping the circuit from establishing. 5) Bit errors could be occurring preventing communication from working. This could be due to bad cables or a bad connection.
SEVERITY	MAJOR
TASK	TP
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	To check for the possible problems named above, take the associated action listed below: 1) Check the PSTN connections at the Remote Office unit. 2) Confirm that the RLC's data port is enabled. 3) Confirm that BRI connections between a 9150 unit and its RLC are 64K clear channel (the required path). 4) Confirm that the correct numbers are configured on both ends. 5) Confirm that cables and connections on both ends are good.
PARAMETERS	N/A
DISPLAYED TEXT	PSTN connection failed to initialize.

Statistic	Definition
LOG NUMBER	64
DESCRIPTION	This log indicates that the unit attempted a PSTN connection to its peer unit at too slow a bit rate. This severely damages system performance since all bandwidth calculations are incorrect.
SEVERITY	Major
TASK	TP
PRODUCT	RLC, 9150
CANCELLATION	None
ACTION TO BE TAKEN	The PSTN path between a 9150 and RLC requires a clear 64k channel. If this log occurs every time a PSTN call is made, then ■ either the wrong service has been ordered from the telephone company. ■ the telephone company has provided the wrong service. If this log occurs intermittently then the connection through the central office has encountered some sort of problem. It is still possible, however, that the wrong service has been ordered, or provided, and that the majority of the time the PSTN has had a clear channel by chance. Some customers have reported that they requested the 64k channel, but a 54k channel was provided instead. Another possible scenario is that bit errors could be occurring, preventing communication from initializing at 64k, but allowing 56k. This is probably the least frequent cause.
PARAMETERS	Unit ID of the unit that tried to connect.
DISPLAYED TEXT	PSTN connection initialized at 56k clear channel unavailable.

Statistic	Definition
LOG NUMBER	65
DESCRIPTION	This log indicates that the unit attempted a PSTN connection to its peer unit, and that the connection attempt succeeded initially at 56K, failed at 65K, and then failed again at 56K.
SEVERITY	MAJOR
TASK	TP
PRODUCT	RLC, 9150
CANCELLATION	None
ACTION TO BE TAKEN:	This problem is most likely related to log number 64 where a clear 64k channel could not be obtained. It is possible that the attempt to increase speed to 64K caused a problem with the central office, making it impossible to re-establish at 56K. This would increase the likelihood of the problem being due to a high bit error rate on the link.
PARAMETERS	N/A
DISPLAYED TEXT	PSTN connection failed to re-initiate at 56K

Statistic	Definition
LOG NUMBER	66
DESCRIPTION	This log indicates that the database has been converted from an older version to the current version. The start and end versions are specified. The status of the conversion is also available.
SEVERITY	NORMAL
TASK	MMI
PRODUCT	9150
CANCELLATION	None
ACTION TO BE TAKEN:	If the status is Failure, user must re-configure the system.
PARAMETERS	1) Status 2) Starting version (From version) 3) Current version (To version)
DISPLAYED TEXT	Database Conversion: P1

Statistic	Definition
LOG NUMBER	67
DESCRIPTION	This log indicates that a locally-defined feature clashes with a PBX defined feature.
SEVERITY	NORMAL
TASK	Device Control
PRODUCT	RLC, 9150
CANCELLATION	None
ACTION TO BE TAKEN:	1. In the case of failure, check the key configurations on the switch and the key configurations done on the 911x, 9150, IDVR for the port concerned. 2. In case of clash Redefine the local feature on a key which is not being used for a PBX feature.
PARAMETERS	1. Remote Office unit Port Number 2. Key Number
DISPLAYED TEXT	Port P1: Local Feature Overrides PBX Feature on key P2.

Statistic	Definition
LOG NUMBER	68
DESCRIPTION	This log indicates that a PSTN connectivity test has started to a specified remote, in a specified mode.
SEVERITY	NORMAL
TASK	Network Manager
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN:	None
PARAMETERS	1. Remote board ID 2. Mode in which test started. a. Disruptive test b. Non disruptive test
DISPLAYED TEXT	PSTN connectivity test started for remote = P1, in mode = P2

Statistic	Definition
LOG NUMBER	69
DESCRIPTION	This log indicates that a PSTN connectivity test is completed or aborted.
SEVERITY	NORMAL
TASK	Network Manager
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN:	None
PARAMETERS	1. Remote board ID 2. Test ended manner a. Normal end b. Aborted
DISPLAYED TEXT	PSTN connectivity test ended for remote = P1 and P2

Statistic	Definition
LOG NUMBER	70
DESCRIPTION	This log indicates that there was a failure in adding a DN to the system, since the DN was already in the system. If you want to place a local call to this set, you must use the number configured through Configuration Manager.
SEVERITY	NORMAL
TASK	Device Control
PRODUCT	9150
CANCELLATION	None
ACTION TO BE TAKEN:	Do not configure MADN on the primary key if both of the sets are on the 9150.
PARAMETERS	1. Remote Office unit Port Number 2. DN which couldn't be added to the system.
DISPLAYED TEXT	MADN Conflict for DN P1 on Port P2: Could not update local DN.

Statistic	Definition
LOG NUMBER	71
DESCRIPTION	This log indicates that the PBX has returned an Illegal number error when attempting to dial from the Network port on the RLC to the 9150 Remote Office unit. Most frequently, this error occurs when the dialed number is going to be routed by the PBX, or Central Office, over an analog trunk instead of a clear channel data path.
SEVERITY	MAJOR
TASK	DL
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN:	1. Verify that the Network port is configured correctly on the PBX 2. Verify that the number dialed from the RLC to the 9150 is correct. 3. Verify that the PBX trunks used allow clear channel data. LD 80 traces of the data port are helpful. 4. Verify that central office is not routing the data call over voice circuits.
PARAMETERS	1. Network port from which this call was placed 2. Last number dialed by a Network port, usually this port.
DISPLAYED TEXT	Network Port P1 call to P2 may be routed over Voice circuits.

Statistic	Definition
LOG NUMBER	72
DESCRIPTION	This log indicates that a key map update is written into the Flash.
SEVERITY	NORMAL
TASK	MMI
PRODUCT	9150
CANCELLATION	None
ACTION TO BE TAKEN:	None
PARAMETERS	Status - SUCCESS if Save to Flash is successful. Status - FAILED if the flash save attempt failed.
DISPLAYED TEXT	Key Map Save to Flash: P1

Statistic	Definition
LOG NUMBER	73
DESCRIPTION	This log indicates an invalid compression type (e.g., G729/Fax or G726) has been configured for the 911x. It is then reset to G729.
SEVERITY	MINOR
TASK	MMI
PRODUCT	911x
CANCELLATION	None
ACTION TO BE TAKEN:	None
PARAMETERS	P1: Remote Site Number P2: Port Number. Status - FAILED if the flash save attempt failed.
DISPLAYED TEXT	"Remote Site: P1[911x] registered to Port P2with Invalid Compression, reset to G729

Statistic	Definition
LOG NUMBER	74
DESCRIPTION	This log indicates a status change (e.g, UP/DOWN) for the BRI line.
SEVERITY	NORMAL
TASK	MMI
PRODUCT	9150
CANCELLATION	None
ACTION TO BE TAKEN:	None
PARAMETERS	P1: Describes status change (e.g, UP) P2: BRI Module Number
DISPLAYED TEXT	P1 detected for BRI Module P2.

Statistic	Definition
LOG NUMBER	75
DESCRIPTION	This log indicates the system is not able to bring up an analog line due to non-availability of modem DSPs.
SEVERITY	MINOR
TASK	MMI
PRODUCT	9150
CANCELLATION	None
ACTION TO BE TAKEN:	a) Ensure that enough Modem channels are configured on DSPs
PARAMETERS	P1: Remote Unit ID
DISPLAYED TEXT	Not able to connect remote: P1 on modem due to non availability of Modem channels

Statistic	Definition
LOG NUMBER	76
DESCRIPTION	This log indicates that the software version of the remote unit is incompatible with the software version installed in the unit generating this message.
SEVERITY	MAJOR
TASK	MMI
PRODUCT	9150, RLC, 911x
CANCELLATION	None
ACTION TO BE TAKEN:	Verify software versions on both units.
PARAMETERS	P1: Remote Unit ID
DISPLAYED TEXT	Communication with Remote P1 is not possible due to software incompatibility

Statistic	Definition
LOG NUMBER	77
DESCRIPTION	This log indicates that the RLC's remote unit config does not match the remote device that is initiating the call. This is probably due to a config error.
SEVERITY	MAJOR
TASK	MMI
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN:	Verify Remote Unit configuration
PARAMETERS	P1: Remote Unit ID
DISPLAYED TEXT	Remote Unit = P1 is found to be of incompatible board type. Communication not possible

Statistic	Definition
LOG NUMBER	78
DESCRIPTION	This log indicates that the keymap version of the PBX software has changed. This is normal when upgrading major PBX versions.
SEVERITY	NORMAL
TASK	MMI
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN:	None
PARAMETERS	P1, P2: Keymap database version P3: Indicates Success or Failure
DISPLAYED TEXT	PBX Model database conversion from Ver P1 to Ver P2 P3

Statistic	Definition
LOG NUMBER	79
DESCRIPTION	This log indicates the status of the keymap flash read.
SEVERITY	NORMAL
TASK	MMI
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN:	None
PARAMETERS	P1: SUCCESS or failure reason.
DISPLAYED TEXT	P3 PBX Model database read - P1

Statistic	Definition
LOG NUMBER	80
DESCRIPTION	This log indicates that connectivity on the specified medium to the specified remote unit closed. This is a part of normal system operation.
SEVERITY	NORMAL
TASK	Network Manager
PRODUCT	RLC, 9150, 911x
CANCELLATION	None
ACTION TO BE TAKEN	None
PARAMETERS	1) Remote unit 2) Medium (ISDN, IP)
DISPLAYED TEXT	Connectivity is closed to Remote: P1 on Media: P2

Statistic	Definition
LOG NUMBER	81
DESCRIPTION	This log indicates that connectivity on the specified medium to the specified remote failed abnormally due to an unspecified problem on the network.
SEVERITY	MAJOR
TASK	Network Manager
PRODUCT	RLC, 9150, 911x
CANCELLATION	A message that indicates that signaling is up on the specified medium.
ACTION TO BE TAKEN	Check for the following on the specified medium: 1) Network connectivity both at RLC and the remote site 2) Check if any problem arose anywhere else on the network between RLC and the remote 3) Check if any of the units got reset for any reason.
PARAMETERS	1) Remote unit 2) Medium (ISDN, IP)
DISPLAYED TEXT	Abnormal failure of connectivity on Media: P1 to Remote: P2

Statistic	Definition
LOG NUMBER	82
DESCRIPTION	This log indicates that Network Manager task states for a particular remote unit got reset and all the connections to the remote are cleared. This can happen due to the following reasons: 1) An error occurred in the system to automatically trigger Network Manager reset 2) User has issued a debug command "nmr x" where x is a valid remote unit number.
SEVERITY	MAJOR
TASK	Network Manager
PRODUCT	RLC, 9150, 911 x
CANCELLATION	None
ACTION TO BE TAKEN	System should work normally after the log is displayed. If not, contact Technical support personal for help. If the log is displayed too frequently, check if anyone is entering debug commands. If not, contact technical support.
PARAMETERS	Remote unit
DISPLAYED TEXT	States reset in NM for Remote: P1

Statistic	Definition
LOG NUMBER	83
DESCRIPTION	This log indicates the result of DN discovery on RLC. If the result in the log is Failure or Partial Success then the system retries for up to five times at three minute intervals if port(s) is (are) busy during first attempt. The system records the status of the initial attempt as well as the last attempt, if made.
SEVERITY	NORMAL
TASK	Call Processing
PRODUCT	RLC
CANCELLATION	None
ACTION TO BE TAKEN	Ensure that LOG shows SUCCESS after every DN Discovery session (either triggered by time-of-day or manually). In case of FAILURE / PARTIAL SUCCESS, check if DN Discovery port is idle, not in set busy, or call forwarded state.
PARAMETERS	Status: SUCCESS, PARTIAL SUCCESS, FAILURE
DISPLAYED TEXT	DN Discovery has completed: result - P1

Glossary

10BaseT Ethernet

The Ethernet standard for baseband local area networks using twisted-pair cable carrying 10 megabits per second (Mbps) in a star topology.

A

A-law

A companding technique used in encoding and decoding audio signals in 30-channel pulse code modulated (PCM) systems. A-law companding is the primary method used in Europe. *See also* Mu-law.

adapter

Hardware required to support a particular device. For example, network adapters provide a port for the network wire. Adapters can be expansion boards or part of the computer's main circuitry.

administrator

A user who is responsible for maintaining the RLC or its associated remote units.

agent

A person who is responsible for handling customer calls.

analog

The type of signal used by most telephone connections. A modem converts a digital (computer) signal to analog, and vice versa, so that the signal can travel through telephone lines.

API

See application program interface.

application

A program that runs on a computer.

application program interface

A set of routines, protocols, and tools that programmers use to develop software applications. APIs simplify the development process by providing commonly used programming procedures.

Automatic Call Distribution (ACD) applications

A separate system or built-in feature of a PBX that equally distributes incoming calls to agents. As calls come in, they are placed into a queue (or a waiting line) for the next available agent. The RLC and its associated remote units support all of Nortel Networks' ACD applications.

B**bandwidth**

The amount of data that the network can transmit, usually expressed in Mbytes per second.

baseboard

See motherboard.

Basic Input/Output System

Flash ROM-based code that runs the Power-On Self-Test (POST) and bootstrap loader. BIOS contains low-level access routines for hardware that can be called from DOS.

BIOS

See Basic Input/Output System.

bit

Short for binary digit, the smallest unit of information on a machine. A single bit can hold only one of two values: 0 or 1.

branch station

A phoneset or fax machine located at the Remote Office 9150 site.

BRI

Basic Rate Interface. An ISDN subscriber service that uses two B (64 Kbps) channels and one D (64 Kbps) channel to transmit voice, video, and data signals.

bridge

A protocol-independent device that connects two LANs or two segments of the same LAN. Bridges are faster (and less versatile) than routers because they forward packets without analyzing and rerouting messages.

bus

A collection of wires that connects the microprocessor and main memory to internal computer components. All buses consist of an address bus that transfers data and a data bus that transfers information about where the data should go.

In a network, the bus (also called the backbone) is the main cable that connects all devices on a LAN.

byte

Abbreviation for binary term, a unit of storage capable of holding a single character. On almost all modern computers, a byte is equal to eight bits. Large amounts of memory are indicated in terms of kilobytes (1 024 bytes), megabytes (1 048 576 bytes), and gigabytes (1 073 741 824 bytes).

C**cache**

A temporary storage area in computer memory.

call duration timer

Used in circuit-switched mode only, it specifies the minimum length of time that each call to the host PBX remains open, regardless of telephone activity (or lack thereof).

call on demand

A call connection that is opened only when a connection to the host PBX is required. This is different from a permanent connection, which is open all the time.

call treatment

A method of handling applied to a call while it is waiting to be answered or serviced.

Caller ID

Caller ID is used on the RLC to identify the number of the caller requesting access to one of its ports. It is also used on the Remote Office 9150 unit to authenticate incoming calls from the RLC.

Calling Line Identification

An optional service that identifies the telephone number of the caller. This information can then be used to route the call to the appropriate agent or skillset. The caller's telephone number can also be displayed on a phoneset.

card

A thin, rectangular plate on which chips and other electronic components are placed. Examples of cards include motherboards, expansion boards, daughterboards, controller boards, network interface cards, and video adapters.

CD-ROM

A type of optical disk capable of storing large amounts of data (up to 1 Gbyte), although the most common size is 630 Mbytes. A single CD-ROM has the storage capacity of 700 floppy disks and is particularly well-suited to information that requires large storage capacity.

CLAN

See Customer local area network.

CLID

See Calling Line Identification.

client

The part of a client/server architecture that runs on a personal computer or workstation and relies on a server to perform some operations. For example, an e-mail client is an application that enables you to send and receive e-mail.

codec

An acronym for COder-DECoder. A device that codes analog signals into digital signals for transmission and decodes digital signals into analog signals for receiving.

COM or COMM

Communications port. This usually refers to the Logical Device name of PC serial ports as defined by DOS.

computer-based training

Computer-based training (CBT) is a type of education in which students learn by running special training programs on a computer. CBT is especially effective for training people to use computer applications, because the CBT program can be integrated with the applications.

Configuration Manager

The software application used to configure and administer the Remote Office 9150 unit and the RLC to which it is connected.

controller board

A special type of expansion board that contains a controller for a peripheral device. When you attach new devices to a computer, such as a disk drive, often a controller board must also be added.

CPU

Central processing unit. This is the system unit that holds a PC's essential components.

crash

A serious computer failure during which the computer stops working or a program closes unexpectedly. A crash indicates a hardware malfunction or a serious software bug.

Customer local area network

The LAN to which your corporate services and resources connect. The RLC and its associated remote units both connect to the CLAN.

D**daughterboard**

Usually used as a synonym for an expansion board, a daughterboard is any printed circuit board that connects directly or indirectly to a motherboard.

DB-9 connector

A 9-pin connector labeled ADMIN that provides the RS-232 serial port interface. This serial port connection can be used to configure a Remote Office 9150 unit that is directly connected to a PC.

DB-25 connector

A 25-pin connector labeled V.35 provides a V.35 serial port connection for voice and signaling. This connection can be used to send voice traffic over a Frame Relay network instead of an Ethernet network.

Note: On the RLC and Remote Office 9150 unit, the V.35 connector is for future use.

DHCP

See dynamic host configuration protocol.

digital signal processor

A special type of coprocessor that manipulates analog data, such as sound or photographs, that has been converted to digital form.

directory number

The number that identifies a phoneset on a switch. The directory number (DN) could be a local extension (local DN), a public network telephone number, or an automatic call distribution directory number (ACD-DN).

DLL

See dynamic link library.

DN

See directory number.

driver

A program that controls a device. Every device, whether it is a printer, disk drive, or keyboard, must have a driver program. A driver acts like a translator between the device and programs that use the device.

DSP

See digital signal processor.

dynamic host configuration protocol

A protocol for dynamically assigning IP addresses to devices on a network.

dynamic link library

A library of executable functions or data that can be used by a Windows application. Typically, a DLL provides one or more particular functions and a program accesses the functions by creating either a static or dynamic link to the DLL. A DLL can be used by several applications at the same time.

dynamic port pool

A RLC feature that is similar to multi-user ports in that multiple stations can share ports on the RLC. However, users sharing ports from a dynamic pool are assigned to the first available port on the RLC.

E**ECC**

See error correction code.

EEPROM

See electronically erasable programmable read-only media.

ELAN

See embedded local area network.

electronically erasable programmable read-only media

A memory chip that needs only a higher than normal voltage and current to erase its contents. An EEPROM chip can be erased and reprogrammed without taking it out of its socket. An EEPROM chip gives a computer and its peripherals a means of storing data without the need for a constant supply of electricity.

embedded local area network

This is the network connection from the PBX to the RLC. It is an Ethernet LAN that is segmented from the rest of the Ethernet network and enables signaling and administration access to the RLC. Nortel Networks recommends the following:

- IP traffic should not be routed between the main network and the ELAN.
- An IP route should not be established between the two LANs.

Emergency Service Number

The Remote Office 9150 unit allows you to program an emergency service number (such as 911).

EMI

Electromagnetic interference

error correction code

A scheme that can detect and fix single-bit memory errors without crashing the system. Also known as Error Detection and Correction (EDAC).

Ethernet

A widely used LAN protocol that uses a bus topology and supports data transfer rates of 10 Mbps.

event

An occurrence or action on the RLC or remote unit, such as the sending or receiving of a message, the opening or closing of an application, or the reporting of an error. Some events are for information only, while others can indicate a problem.

expansion board

Any board that plugs in to one of the computer's expansion slots. Expansion boards include controller boards, LAN cards, and video adapters.

expansion bus

Enables expansion boards to access the microprocessor and memory. *See also* bus.

F**first-level threshold**

The value that represents the lowest value of the normal range for a given field in a threshold class. The system tracks how often the value for the field falls below this value.

G

G.711

G.711 is the international standard for encoding telephone audio on a 64 Kbps channel. It is a pulse code modulation (PCM) scheme operating at an 8 kHz sample rate, with 8 bits per sample. According to the Nyquist theorem, which states that a signal must be sampled at twice its highest frequency component, G.711 can encode frequencies between 0 and 4 kHz. Telcos can select between two different variants of G.711: A-law and μ -law. A-law is the standard for international circuits.

G.726

G.726 is a standard ADPCM algorithm specified by the International Telecommunication Union (ITU) for reducing the 64 kbps A-Law or μ -law logarithmic data of a normal telephone line to 16, 24, 32, or 40 kbps.

G.729

G.729 is a voice compression International Telecommunications Union (ITU) standard that can be used in a wide range of applications including wireless communications, digital satellite systems, packetized speech, and digital leased lines. G.729 provides 8 Kbps of bandwidth for compressed speech at toll quality (equivalent to G.726 32 Kbps ADPCM under clean channel condition).

gateway

A device that functions as a node on two or more networks, forwarding packets from one network to addresses in the other networks. In Remote Office context, the gateway is the device on the network that directs traffic to and from the Remote Office 9150 unit or RLC.

Gbyte

1 073 741 824 bytes. One Gbyte is equal to 1024 Mbytes.

general protection fault

A computer condition that causes a Windows application to crash. GPFs usually occur when one application attempts to use memory assigned to another application.

GPCP

General purpose computing platform

GPF

See general protection fault.

graphical user interface

The information displayed on the monitor when a Windows application (or another non-command-based application) runs. A graphical user interface uses features such as pointers, icons, I-beams, and menus to make the program easier to use.

H**handshaking**

A process involved in establishing a valid connection or signal between two pieces of hardware or communications software.

host call appearance key

An assigned key on the telephone set at the remote site that is used to establish a connection with the host PBX or to receive incoming calls from the host PBX.

host-controlled call mode

When a call is placed to someone at the host site, or when someone from the host site calls the remote site, the call is in host-controlled call mode. Calls in host-controlled mode are routed through the PBX.

host station

A telephone set located at the host PBX site.

host trunk

The ISDN PRI or TI connection located at the host site. Host trunks are used to route calls from the host PBX to remote sites over the PSTN.

hub

A common connection point for all 10Base-T cables connected to a small network. A hub enables data to go from one device to another.

I**icon**

A small picture that represents an object or program in a graphical user interface.

idle timer

Identifies the maximum length of time during which an ISDN connection should remain idle before it can be closed. Idle means that a voice connection does not exist, and buttons are not being pressed on the digital telephone.

input/output

Refers to any operation, program, or device that enters data into a computer or extracts data from a computer.

I/O

See input/output.

IP

Internet Protocol. The protocol within TCP/IP that governs the breakup of data messages into packets, the routing of the packets from sender to destination network, and the reassembly of the packets into the original data messages at the destination.

IP address

Internet Protocol address. An identifier for a computer or device on a TCP/IP network. Networks use the TCP/IP protocol to route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be 0–255. For example, 1.160.10.240 can be an IP address.

ISDN

Integrated Services Digital Network. A worldwide digital communication protocol that permits telephone networks to carry data, voice, and other source material. There are two kinds of ISDN lines—Primary Rate Interface (PRI) and Basic Rate Interface (BRI). *See also* BRI.

J**jumper**

A metal bridge that closes an electrical circuit. Typically, a jumper consists of a plastic plug that fits over a pair of protruding pins. Jumpers are sometimes used to configure expansion boards. By placing a jumper plug over a different set of pins, you can change a board's parameters.

K

kbyte
1024 bytes

L

LAN
See Local area network.

LED
Light emitting diode

Local area network
A computer network that spans a relatively small area. Most LANs connect workstations and personal computers and are confined to a single building or group of buildings.

local call
A call that originates at your site.

local call appearance key
An assigned key on the telephone set at the Remote Office 9150 site that is used to call another station at the branch office, or to make and receive calls through the local PSTN.

locally controlled call mode
When you place a call from a specified local call appearance key, or your call is to another telephone at your branch site, you are in locally controlled call mode. Calls in locally controlled mode are routed through the local PSTN.

local station
A telephone set located at the Remote Office 9150 site.

M

M1
Meridian 1 PBX

MAT
Meridian Administration Tools. This is a Nortel Networks software application that is used to administer the Meridian 1 PBX.

Mbyte

1 048 576 bytes

megahertz

One million cycles per second.

MHz

See megahertz.

RLC

An abbreviation for Reach Line Card. The RLC is installed on the host PBX at the host location and relays voice and signaling information from the digital telephones connected at a remote site to the PBX at the host site.

motherboard

The principal board that has connectors for attaching devices to the bus. Typically, the motherboard contains the CPU, memory, and basic controllers for the system. On PCs, the motherboard is often called the system board.

MTBF

Mean time between failures

Mu-law

A companding method for encoding and decoding audio signals in 24-channel pulse-code-modulated (PCM) systems. Mu-law is the method used in North America and Japan. *See also* A-law.

Multi-user ports

A RLC port feature that allows multiple stations to time-share a single port on the host PBX. All stations that use a multi-user port are always assigned to the same port number (TN) on the host PBX.

N

network interface card

An expansion board that enables a PC to be connected to a local area network (LAN).

NIC

See network interface card.

node

A device connected to the network capable of connecting to other network devices. For example, the RLC and Remote Office 9150 unit are both nodes on the network.

NPA

See Number Plan Area.

Number Plan Area

Area code

NVRAM

Non-Volatile Random Access Memory

O**OA&M**

Operations, administration, and maintenance

object linking and embedding

A compound document standard that enables you to create objects with one application and then link or embed them in a second application.

OEM

Original equipment manufacturer

online/offline table

The online/offline table is configured on the RLC. It allows you to schedule times that the host PBX connection is made available to the remote site and at which times all telephones at the remote site can use only the local telephone service.

The online/offline table is used for controlling ISDN BRI costs.

Open System Interconnection

A worldwide communications standard that defines a framework for implementing protocols in seven layers.

OS

Operating Standard

OSI

See Open System Interconnection.

P**packetized voice**

Digital Signal Processors (DSPs), located in the Remote Office 9150 unit and RLC, convert analog voice into digital data. The data is constructed as a UDP/IP voice packet for transmission over an IP network.

parity

The quality of being either odd or even. The fact that all numbers have parity is commonly used in data communications to ensure the validity of data.

PBX

See private branch exchange.

pegging

The action of incrementing statistical counters to track system events.

pegging threshold

A threshold used to define a cut-off value for statistics such as short call and service level. Pegging thresholds are used in reports and historical statistics.

personal directory number

A DN on which an agent can be reached directly, usually for private calls.

ping

Packet Internet Groper. A protocol that can be used to test the Ethernet connection to devices on the network (such as the RLC and its associated remote units).

POST

See Power-On Self-Test.

Power-On Self-Test

Initializes and performs rudimentary tests on baseboard hardware, including CPU, floating point unit, interrupts, memory, real-time clock, video, and auto-initializing PCI and EISA bus.

priority DN

A user station can be configured as a priority DN. There are two levels of priority—high and normal. High priority level allows you to

- ensure a trunk is always available
- use PSTN trunking for the host PBX connections
- move the high priority DN first from the IP network to the PSTN

private branch exchange

A telephone switch, typically used by a business to service its internal telephone needs. A PBX usually offers more advanced features than are generally available on the public network. Users of the PBX share a certain number of outside lines for making telephone calls external to the PBX.

protocol

A standard format used for communication between two devices. The protocol determines the type of error checking to be used, the data compression method (if any), how the sending device indicates that it has finished sending a message, and how the receiving device indicates that it has received a message.

PSTN

Public Switched Telephone Network (also known as the public telephone network).

Q**QoS transitioning technology**

Technology that can automatically switch calls from the IP network to the PSTN when the voice Quality of Service falls below a predetermined threshold, and back to the IP network when the Quality of Service returns to normal.

R

RAM

Random Access Memory. This is the most common type of memory found in computers and other devices, such as printers. The term RAM is usually synonymous with main memory, the memory available to programs. For example, a computer with 8 Mbytes of RAM has approximately 8 million bytes of memory that programs can use.

remote station

A phoneset or fax machine located at the Remote Office 9150 site.

remote trunk

From the RLC's point of view, remote trunks are the ISDN BRI connections between the PSTN and the Remote Office 9150 unit located at the branch office site.

RJ-45 connector

An 8-position, 8-conductor modular jack that provides the 10BaseT Ethernet connection.

ROM

Read-Only Memory. This is the computer memory on which data has been prerecorded and from which it cannot be removed.

router

A device that connects two LANs. Routers are similar to bridges but provide additional functionality, such as the ability to filter messages and forward them to different places based on various criteria.

S

second-level threshold

The value used in display thresholds that represents the highest value of the normal range for a given statistic.

security identifier

The remote unit sends the branch office security identifier (password) to the RLC for each connection request. The RLC matches the identifier configured for the RLC port. When it finds a match, it grants access to the port and allows the call to proceed.

serial port

A general-purpose interface that can be used for almost any type of device, including modems, mice, and printers (although most printers are connected to a parallel port). Most serial ports on personal computers conform to the RS-232C or RS-422 standards.

server

A computer or device on a network that manages network resources. Examples of servers include file servers, print servers, network servers, and database servers.

service

A process that adheres to a Windows NT structure and requirements. A service provides system functionality.

Service Control Manager

A Windows NT process that manages the different services on the PC.

silence suppression

A feature that prevents packet transmission during periods when there is no voice data present.

Simple Network Management Protocol

A set of protocols for managing complex networks. SNMP sends messages called protocol data units (PDUs) to different parts of a network, and then analyzes the responses.

single-user ports

A RLC port that supports one remote station.

SNMP

See Simple Network Management Protocol.

SPID

Service Profile Identifier

SPRE code

A Special Prefix code that is used to initiate use of a PBX feature. In a Remote Office context, SPRE codes are used to

- toggle a remote site between online and offline modes
- use the paging feature
- switch an analog or ATA-equipped station from host-controlled mode to locally controlled mode so that local calls can be made
- register a Remote Office 9150 unit for a multi-user or dynamic port

station

A telephone or fax machine located at a Remote Office 9150 site.

stop bit

In asynchronous communications, a bit that indicates a byte has just been transmitted. Every byte of data is preceded by a start bit and followed by a stop bit.

subnet mask

A subnet mask is the part of the IP address used to represent a subnetwork within a network. A typical IP address might be 192.210.34.144. Each part of this address is made up of eight bits. The subnet mask identifies to the RLC or remote unit what portion of the IP address represents the network (and subnetwork) and what portion represents the host.

switch

In a telecommunications network, a switch is the hardware that receives phone calls and provides connections to phonesets. The switch allows a connection to be established as necessary and terminated when there is no longer a session to support it.

In data networks, a switch is a device that filters and forwards packets between LAN segments. Switches operate at the data link layer (layer 2) of the OSI Reference Model and, therefore, support any packet protocol. LANs that use switches to join segments are called switched LANs or, in the case of Ethernet networks, switched Ethernet LANs.

switch resource

A device that is configured on the switch.

T**TCP/IP**

Transport Control Protocol/Internet Protocol. The communication protocol used to connect devices on the Internet. TCP/IP is the standard for transmitting data over networks.

threshold

A value for a statistic at which system handling of the statistic changes.

threshold class

A set of options that specifies how statistics are treated in reports and real-time displays. *See also* pegging threshold.

trunk

A communications link between a PBX and the public central office, or between PBXs. Various trunk types provide services such as Direct Inward Dialing (DID), ISDN, and central office connectivity.

trunk access code

A trunk access code is a number that is used by the Remote Office 9150 unit to determine which trunk to use when routing a call. For example, 9 is a common trunk access code used to obtain an outside line.

Note: All trunk access codes are configured on the Remote Office 9150 unit with a pound sign (# in North America) so that there are no conflicts with host PBX numbering plans.

trunk groups

A trunk group consists of one or more trunk lines that are logically grouped. You can configure up to eight trunk groups on the Remote Office 9150 unit.

trunk interface modules

Used to route calls over the PSTN. The number of modules you must install on the Remote Office 9150 unit depends on the number of simultaneous calls you want in host-controlled or locally controlled mode.

U**uninterruptible power supply**

A power supply that includes a battery to maintain power in the event of a power outage. Typically, a UPS keeps a computer running for several minutes after a power outage, enabling you to save data that is in RAM and to shut down the computer safely.

UPS

See uninterruptible power supply.

utility

A program that performs a specific task, usually related to managing system resources. Operating systems contain a number of utilities for managing disk drives, printers, and other devices.

V**V.35**

An ITU-T standard describing a synchronous, physical layer protocol used for communications between a network access device and a packet network. V.35 is most commonly used in the United States and in Europe, and is recommended for speeds up to 48 Kbps. In practice, V.35 is used for synchronous transmission up to 2048 Mbps.

V.35 interface

The V.35 interface is for future use.

voice compression

Prior to transmission, the voice data is compressed; after transmission, the data is converted back to voice data at the destination. Voice compression means that voice consumes less bandwidth, leaving more bandwidth for data or other voice or fax communications.

voice jitter attenuation

A feature that removes the variable delays from the voice packets sent across the IP network, thus avoiding awkward-sounding speech.

Voice over IP (VoIP)

Technology that uses the IP data network to carry the voice conversation and telephone set control signals between a remote site and the host PBX.

W**WAN**

Wide area network. A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local area networks (LANs). The largest WAN in existence is the Internet.

Fields index

A

- Add on Module Type 228
- Auto Hold 228, 233

B

- B Channel 218
- B Channel Usage 134
- Bandwidth (BW) Connection Statistics
 - IP QoS Status 283
 - No of Voice Calls on IP 283
 - No of Voice Calls on PSTN 283
 - Remote Unit Number 283
 - Signaling Status 283
 - Total Up Trunk BW 283
 - Used IP BW 283
 - Used Trunk BW 283
- Block Incoming Local Call on Primary B Channel 201
- Bridge Port 228, 233
- Browse (button)
 - Software Upload 318
 - Upload Configuration 269

C

- Call BW 285
- Call Duration 298
- Call Number 285
- Call Start Time
 - Local Call Statistics 298
 - Remote Call Statistics 300
- Call Type 281
- Called Number 281

- Caller ID 206
- Caller Info Statistics
 - Call BW 285
 - Connection ID 285
 - Current Media 285
 - Last Transition to IP 286
 - Last Transition to PSTN 286
 - Priority 285
 - Remote ID 285
 - Start Time 285
 - Transitions to IP 285
 - Transitions to PSTN 285
 - Type 285
- Compression algorithms 237
- Connection ID 285, 300
- CPND 228
- Current Media 285

D

- Default (button) 153
- Device 218
- Disabled Outbound Digit Seq. 229
- DN 233
- DSP Callback pointer 300
- DSP load 237
- Duration 281
 - Remote Call Statistics 300

E

- Emergency Activation Code 186
- Enter a node name to recognize the unit 130
- Enter the local IP Address of the unit 131
- Enter the Local IP Gateway of the unit 131

Enter the Local IP Mask of the unit 131
Enter the PSTN Number 134
Enter the SPID Number 134
Error % 307

F

Forward Busy/No Answer 228, 233
 Number of Rings before transfer 229
 Transfer to DN 229

G

Group No 217

H

Hardware Statistics
 Module No 288
 Module Type 288
 Status 288
 Version 288
Hardware statistics
 Available Channels 290
 Available Flex Channels 291
 Available MIPS 290
 Available Voice Channels 290
 Device Number 290
 In Service 290
 Module Number 290
 Name 291
 Single Dig Dev ID 290
 Total Channels 290
 Total Flex Channels 291
 Total MIPS 290
 Total Reserved Channels 291
 Total Tones Channels 291
 Total Voice Channels 290
Help (button) 154
Hour 306

I

International Tones
 Cadence Time 193
 End Repeat 193
 No of Cycles 193
 Tone Code 193
 Tone Type 193
IP Address
 IP Configuration 196
 RLC Connection Configuration 200
 Software Upload 317
 Upload Configuration 269
IP Connection 200
IP Gateway 196
IP Network Mask 196
IP QoS Status 283
IP Signaling 200
ISDN Line Type 213

L

Last Transition to IP 286
Last Transition to PSTN 286
Local Call Keys 229, 234
Local CPND 233
Local DN 228
Local DNs to Alert 217
Local SwitchOver 189

M

Module
 Software Upload 317
 Trunk Group B-Channel 218
Module # 213
Module Number 237
Module Status 134

N

- New Password 263
- No of Voice Calls on IP 283
- No of Voice Calls on PSTN 283
- Node Name 186
- Number of devices 237

O

- OK (button) 153, 159, 163
- Old Password 263
- Optional Feature Keys 230

P

- Paging 228, 233
- Phone Type 228
- Port No.
 - Local Call Statistics 298
 - Remote Call Statistics 300
- Port Type 226, 232
- Priority 285
- Provision ID 207
- PSTN Connection 200
- PSTN Number 214

R

- RCM Callback pointer 300
- Remote ID 281, 285
 - Caller Info Statistics 285
- Remote Unit Number 283
- Retrieve (button) 154, 160, 163
- Retype New Password 263
- RLC ID 300
- RLC Port 226, 233
- RLC Port No. 300
- Rx Dropped 307
- Rx Error 307
- Rx Frames 307

S

- Security Level 205
- Select the Country Type 134
- Select the Protocol Type 134
- Send (button) 153, 160, 163
- Set the unique Unit ID of the unit 130
- Set the Unit ID of the RLC to connect to 132
- Signaling Status 283
- SPID 214
- SPRE Codes
 - DeRegistration 188
 - Local Calling 188
 - Offline 187
 - Online 187
 - Paging 187
 - Registration 187
- Start Time 281, 285
- statistics
 - Bandwidth (BW) Connection Statistics
 - IP QoS Status 283
 - No of Voice Calls on IP 283
 - No of Voice Calls on PSTN 283
 - Remote Unit Number 283
 - Signaling Status 283
 - Total Up Trunk BW 283
 - Used IP BW 283
 - Used Trunk BW 283
 - Caller Info Statistics
 - Call BW 285
 - Connection ID 285
 - Current Media 285
 - Last Transition to IP 286
 - Last Transition to PSTN 286
 - Priority 285
 - Remote ID 285
 - Start Time 285
 - Transitions to PSTN 285
 - Transitions to IP 285
 - Type 285
 - Trunk Connection Statistics
 - Call Type 281
 - Called Number 281

- Duration 281
- Remote ID 281
- Start Time 281
- Status 281
- Trunk Number 281

- Status 281
 - BRI Configuration 213
 - Trunk Group Configuration 217
- Switch Type 213

T

- Time Offset 186
- Total Up Trunk BW 283
- Total Voice Channels 290
- Transitions to IP 285
- Transitions to PSTN 285
- Trunk Access Code 217
- Trunk Connection Statistics
 - Call Type 281
 - Called Number 281
 - Duration 281
 - Remote ID 281
 - Start Time 281
 - Status 281
 - Trunk Number 281
- Trunk Group B Channels 218
- Trunk Number 281
- Tx Frames 307
- Type 213, 285

U

- Unit ID
 - 9150 System Configuration 186
 - RLC Connection Configuration 200
- UPkts 294
- Used IP BW 283
- Used Trunk BW 283

W

- Which module would you wish to configure 134
- Wish to configure Multiple 9150 Ports 133
- Wish to Enable IP Voice Connection to Remote 132
- Wish to Enable PSTN Connection to RLC 132

Index

Numerics

- 10BaseT Ethernet
 - as a component 2
 - connection option 17
- 25-pair connector 13
- 9150 Port Configuration property sheet 225

A

- add-on modules
 - DSP application modules 16
 - trunk interface modules 15
- Admin 293
- Admin connector pin-out table 379
- administration
 - backups and restores, performing 265
 - password, changing 260
 - Configuration Manager 260
 - Remote Office 9150 unit 262
 - PC
 - connection options 61
 - Meridian Administration Tools and Configuration Manager 65
 - software
 - command line interface 49
 - Configuration Manager 48
 - connection options 48
 - statistics, viewing 279
 - upgrades, performing 309
- analog port 18
 - configuring 232
- ATA equipped stations 224
- Auto Hold 228, 254
- auto logoff 170
- Automatic Call Distribution (ACD) applications 36

B

- backup
 - configuration file, creating 266
- bandwidth
 - allocating 72
 - allocation, description 32
 - extra 43
 - priority reserved 43
- Bandwidth Connection statistics 282
- BRI Configuration property sheet 211
- Bridge Ports 219

C

- call appearance keys
 - defined 222
 - host call appearance key 241
 - local call appearance key 241
- call blocking 68
 - calculating system requirements 69
 - defined 68
 - reducing between Remote Office 9150 unit and host PBX 69
- Call Forward 228, 256
- Call Transfer 255
- Call Waiting 254
- caller identification (security level) 30
- Caller Information statistics 284
- calling permissions and restrictions 223
- calls
 - emergency service 253
 - host-controlled calls 245
 - methods for placing outgoing calls 245
 - outgoing locally controlled calls 246
 - placing 244
 - receiving 244
 - station-to-station calls 247
- Channel 293

- circuit only priority 42
- circuit-switched mode, implementing 83
- clearing logs 277
- components
 - 10BaseT Ethernet connection 2
 - Digital Signal Processor (DSP) 2
 - ISDN BRI trunk interface modules 2
 - Reach Line Card (RLC) 2
 - Remote Office 9150 unit 2
- compression algorithms 37, 74
 - and ATA devices 224
 - and MCA devices 224
- Computer Telephony Integration (CTI)
 - applications 35
- Conference calling 256
- configuration
 - backup
 - creating 266
 - when to create 266
 - DSP Configuration property sheet 235
 - recommendation 360
 - samples
 - Meridian 1 data port 364
 - Meridian 1 voice port 362
 - Remote Office 9150 370
 - RLC 366
- Configuration Manager
 - check boxes 151
 - closing 180
 - command buttons 153
 - configuration
 - downloading 166
 - uploading 166
 - configuration file
 - creating 164
 - opening 165
 - description of 9
 - device type, selecting 167
 - file operations
 - description 159
 - diagram 156
 - logging off from a unit 176
 - logging on to a unit 169
 - menus 147
 - option buttons 151
 - parts of the screen 147
 - password 260
 - property sheets 148
 - scroll boxes 152
 - shutdown, performing 177
 - starting 144
 - system restart, performing 177
 - system tree 148
- Configuration Wizard
 - how it works 124
 - introduction 124
 - starting 125
- configuring Remote Office 9150 unit
 - 9150 Port Configuration sheet 225, 232
 - BRI Configuration sheet 211
 - BRI trunks, configuring 211
 - Cadence Time 193
 - Companding Algorithm 189
 - emergency number 186
 - End Repeat 193
 - fax station, defining 231
 - International Tones 190
 - IP addresses 196
 - local switchover 189
 - Multiple Subscriber Number 189
 - No of cycles 193
 - RLC Connection Configuration sheet 198
 - RLC connection information 198
 - security level 204
 - SPRE codes, defining 187–188
 - system identification information 186
 - Tone Code 193
 - Tone type 193
 - Trunk Group Configuration sheet 215
 - trunk groups, configuring 215
- connecting the Remote Office 9150 unit
 - cables you must provide 113
 - connection panel diagram 115
 - pin-out references 114
- connection bandwidth
 - extra bandwidth 43
 - priority reserved bandwidth 43
- connection history 170
- connection options
 - 10BaseT Ethernet interface 17
 - analog port for fax machines 18
 - ethernet connection 62

- IP Quality of Service transitioning technology 17
- ISDN BRI lines to PSTN 17
 - serial connection 61
- connection types 32
- connector pin-outs
 - Admin 379
 - Ethernet 378
 - Power 380
 - Telco 1 374
 - Telco 2 376
- connectors
 - 25-pair 13
 - DB-25 13
 - DB-9 13
 - RJ-45 13
- cover, removing the Remote Office 9150 97

D

- DB-25 connector 13
- DB-9 connector 13
- deploying Remote Office 9150 unit
 - circuit-switched mode, implementing 83
 - overview 82
 - port and station assignment 82
 - Quality of Service transitioning technology 85
 - Voice over IP mode, implementing 84
- device connectivity 330
- Digital Signal Processor (DSP) 2
- digital telephones
 - display messages 250
 - supported 35
 - troubleshooting 325
- Disabled Outbound Digit Seq. 229
- Disc 293, 294
- display messages 250
- displaying logs 274
- DLL files 123
- documentation, related
 - Meridian 1 xvii
 - MIG RLC xvii
 - obtaining xviii
 - Remote Office 9150 xvii

- Download Configuration 162, 163
- DSP
 - DSP Configuration property sheet 235
- DSP modules
 - adding 79
 - installing 103
 - removing 103
 - what they do 100
 - when to install 101
 - where they can be installed 101
- DSP Statistics 290
- DSP Statistics screen 289
- dynamic port pooling 40

E

- electrostatic discharge 93
- emergency
 - activation code
 - description of 47
 - calls, placing 253
 - service calls 253
 - service number 186
- EPROM checksum validation 119
- Err 293, 294
- Ethernet
 - connector pin-out table 378
 - LED 12
- Ethernet Interface Statistics
 - Admin 293
 - Channel 293
 - Disc 293, 294
 - Err 293, 294
 - IFC No 293
 - IFC Type 293
 - In - Octet 293
 - LAN Drv 293
 - MPkts 293, 294
 - MTU Len 293
 - Oper 293
 - Out - Octet 294
 - QLen 294
 - Speed 293
 - UPkts 293
- extra bandwidth 43

F

- fax port, configuring 232
- fax support 47
- File Open 159, 163
- File Save As 159, 163
- firmware
 - types of 312
 - upgrade files
 - downloading 312
 - extracting 313
 - upgrade, performing 315
 - version, verifying 310
- flash checksum validation 119
- future growth
 - DSP modules, adding 79
 - maximum configurations 80
 - trunk interface modules, adding 80

G

- general safety
 - electrostatic discharge safety precautions 93
 - introduction 92
 - precautionary messages 92
 - safety precautions 92
- GUI
 - DSP Configuration property sheet 235

H

- hardware description
 - connectors 13
 - LEDs 11
 - mounting options 13
 - universal power supply 13
- hardware installation tools 94
- Hardware Statistics 287
- host-controlled mode 240
 - and Call Transfer feature 255
 - and Call Waiting feature 254
 - and Hold feature 254
 - calls, placing 245
 - external corporate call, example 24
 - indicator updates 248

internal corporate call, example 22

I

- idle timer 33
- IFC No 293
- IFC Type 293
- In - Octet 293
- incoming call process 20
- incoming calls, receiving 244
- indicators, telephone
 - host-controlled indicator updates 248
 - introduction 248
 - locally controlled indicator updates 248
- installing the Remote Office 9150 unit
 - Configuration Wizard 124
 - connecting 113
 - cover, removing 97
 - general safety 92
 - mounting 106
 - network connections, testing 138
 - powering up 119
 - required tools 94
 - software, installing 122
 - unpacking and inspecting 95
- interface loopbacks 119
- International Tones 190
- IP
 - addresses 89
 - addressing and routing 66
 - interface, configuring 195
- IP Configuration property sheet 196
- IP only priority 41
- ISDN BRI
 - BRI Configuration sheet 211
 - connection option 17
 - planning for 88
 - trunks groups, configuring 215
 - trunks, configuring 211

K

- Key Feature Configuration property sheet 230

L

LAN Drv 293

LEDs

- Ethernet 12

- Module 12

- Power 12

- Status 12

- troubleshooting 323

- V.35 12

- when powering up 119

local calling

- Bridge Port 45

- call restrictions 45

- local calls through PSTN 45

- local extension calling 44

- telephone features

 - supported 45

 - unsupported 45

Local Profile Configuration property sheet 227

local switchover 189

locally controlled mode 21, 241

- and Call Transfer feature 255

- and Call Waiting feature 254, 255

- and Hold feature 254

- calls, placing 246

- indicator updates 248

- local call, example 26

logging off from a unit 176

- auto logoff 170

logging on to a unit

- connection history 169, 170

- connection types 169

- default logon ID and password 169

- from Configuration Manager 169

- through serial port 174

- through Telnet 172

logon ID (to a unit) 169

logs

- clearing 277

- displaying 275

- overview 273

- printing 275

- resizing 276

M

MCA equipped stations 224

Meridian 1

- data port configuration (example) 364

- voice port configuration (example) 362

Meridian Administration Tools (MAT) 65

messages, telephone display 250

minimum call duration timer 33

Module LEDs 12

mounting the Remote Office 9150 unit

- choosing a suitable location 106

- installing in a rack 110

- installing on a desk 107

- installing the unit on the wall 108

MPkts 293, 294

MSN 189

MTU Len 293

multi-user ports 40

N

network

- connecting the Remote Office 9150 unit to 117

- considerations

 - call blocking 68

 - IP addressing and routing 66

 - network diagram 67

 - numbering plans 68

 - Quality of Service 67

- diagram (example) 361

no security (security level) 30

normal priority 41

O

offline mode

- defined 242

- importance of 242

- what controls offline mode 242

OK 159, 163

online help (accessing) 155

online mode

- defined 242

- what controls online mode 242
- online/offline
 - automatic offline event, overriding 258
 - scheduling 71
 - SPRE codes, using 257
- online/offline mode
 - changing 71
 - offline, description 242
 - online, description 242
- online/offline table
 - configuration 46
 - description 46
 - how the table works 46
- Oper 293
- optional modules
 - DSP application module 16
 - trunk interface module 15
- Out - Octet 294
- outgoing calls, placing 244
 - description 20

P

- packet loss handling techniques 37
- Paging 228, 256
- password (for a unit) 169
- PC
 - connection options 61
 - Meridian Administration Tools and Configuration Manager 65
- physical environment 56
 - cables, included 59
 - cables, not included 59
 - connections 58
 - mounting options 58
- Ping, using 336
- pin-out tables, connector
 - Admin 379
 - Ethernet 378
 - Power 380
 - Telco 1 374
 - Telco 2 376
- planning
 - configuration 87
 - data entry form completion sequence 87

- deployment options 82
- future growth 79
- network considerations 66
- numbering plan 90
- online/offline schedule 89
- physical environment 56
- security 77
- station configuration 73
- trunk configuration 90
- trunk connection management 70
- port management
 - dynamic port pool 40
 - multi-user ports 40
 - single-user ports 40
- ports, types of 75
- Power
 - connector pin-out table 380
 - LED 12
- precautionary messages 92
- priority level
 - circuit only priority 42
 - IP only priority 41
 - normal priority 41
- priority reserved bandwidth 43
- private lines, creating 222
- Provision ID (security level) 30

Q

- QLen 294
- Quality of Service transitioning technology
 - connection option 17
 - defined 39
 - implementing 85
 - log reports and statistics 39
 - transport connections 39

R

- rack installation 110–112
- RAM memory test 119
- Reach Line Card
 - as a component 2
 - configuration (example) 366
 - description of 8

- related documentation
 - Meridian 1 xvii
 - MIG RLC xvii
 - obtaining xviii
 - Remote Office 9150 xvii
- Remote Call Statistics 299
- remote configuration
 - configuring the remote connection settings 236
 - property sheet 235
- Remote Office 9150 unit
 - add-on modules 15
 - administering 259–320
 - as a component 2
 - cables you must obtain 113
 - configuration (example) 370
 - Configuration Wizard 124
 - configuring ??–234
 - connecting to the network 117
 - connection options 17
 - cover
 - removing 97
 - replacing 99
 - description 8, 9, 11
 - how it works 19
 - LEDs 323
 - mounting 106
 - network connections, testing 138
 - password, changing 262
 - port management 40
 - powering up 119
 - software, installing 122
 - station priority and connection bandwidth 41
 - stations, using 239–258
 - troubleshooting 322
- restarting the system
 - performing a restart 177
 - when to perform a restart 177
- restoring the configuration
 - before you begin 268
 - upload, performing 268
- Retrieve 160, 163
- RJ-45 connector 13
- RLC Connection Configuration property sheet 198

S

- safety precautions 92
- Save to Flash 160
- security
 - data network security 77
 - description 77
 - identifier 30, 204
 - RLC Connection Configuration sheet 202, 205
 - security level, configuring 204
 - system configuration 78
 - toll fraud 77
- Send 160, 163
- Send All 160, 163
- serial port, logging on to a unit 174
- shutting down the system
 - performing a system shutdown 178
 - when to perform a shutdown 177
- silence suppression 38
- single-user ports 40
- software
 - installing 122
 - troubleshooting 334
 - upgrades
 - performing 320
 - version, verifying 310
- Speed (statistic) 293
- SPRE codes
 - configuring 187–188
 - controlling online and offline modes 243
- stations
 - 9150 Device Configuration sheet 225
 - assignment and configuration 87
 - ATA and MCA-equipped stations and bandwidth requirements 224
 - call appearance keys 222
 - call processing capabilities and station settings 220
 - calling permissions and restrictions 223
 - configuration overview
 - Remote Office 9150 settings 75
 - RLC setting 73
 - Configuring Bridge Ports 219
 - defining 225
 - display messages 250

- going online and offline 257
 - modes
 - controlling online and offline 242
 - host-controlled 240
 - importance of 242
 - locally controlled mode 241
 - of operation 240
 - offline mode 242
 - online mode 242
 - relationship between host-controlled and locally controlled modes 241
 - placing and receiving calls 244
 - priority
 - circuit only priority 42
 - IP only priority 41
 - normal priority 41
 - private lines 222
 - telephone features 253
 - telephone indicators 248
 - station-to-station calls 247
 - statistics
 - Bandwidth Connection Statistics screen 282
 - Caller Information Statistics screen 284
 - DSP Statistics screen 289, 290
 - Ethernet Interface Statistics
 - Admin 293
 - Channel 293
 - Disc 293, 294
 - Err 293, 294
 - IFC No 293
 - IFC Type 293
 - In - Octet 293
 - LAN Drv 293
 - MPkts 293, 294
 - MTU Len 293
 - Oper 293
 - Out - Octet 294
 - QLen 294
 - Speed 293
 - UPkts 293
 - Hardware Statistics screen 287
 - overview 279
 - Remote Call Statistics screen 299
 - Trunk Connection Statistics screen 280
 - viewing 279
 - Status LED 12
 - System Configuration sheet 184
 - system security
 - caller identification 30
 - no security 30
 - security identifier 30
 - system tree 148
- ## T
- Telco 1, connector pin-out table 374
 - Telco 2, connector pin-out table 376
 - telephone features
 - Call Forward 256
 - Call Transfer 255
 - Call Waiting 254
 - Conference 256
 - emergency service calls 253
 - Hold 254
 - Paging 256
 - telephone modules (supported) 35
 - telephones
 - Automatic Call Distribution (ACD) 36
 - Computer Telephony Integration (CTI)
 - applications 35
 - digital telephones 35
 - supported modules 35
 - See also* stations
 - Telnet, using to log on to unit 172
 - TFTP
 - and upgrades 315
 - server 64
 - tools required
 - hardware installation tools 94
 - software installation or upgrade tools 94
 - troubleshooting
 - before you begin 322
 - device connectivity 330
 - digital telephone 325
 - overview 322
 - Ping option 336
 - recovering from a catastrophic failure 339
 - Remote Office 9150 LEDs 323
 - software problems 334
 - trunk access codes 209
 - Trunk Connection Statistics 280

- trunk connections 32
 - bandwidth allocation 72
 - changing online/offline mode 71
 - online/offline schedule 71
 - QoS transitioning technology 70
- Trunk Group Configuration property sheet 215
- trunk groups 209
 - configuring 215
 - trunk access codes 209
- trunk groups, configuring 215
- trunk interface modules
 - adding 80
 - installing 103
 - removing 103
 - what they do 100
 - when to install 101
 - where they can be installed 101
- trunking
 - and idle timer 33
 - and minimum call duration timer 33
 - bandwidth allocation 32
 - connection types 32
 - types 32
- trunks
 - configuring 211
 - local and remote trunk 208
 - local trunk 208
 - managing trunk connections 70
 - remote trunk 208
 - trunk access codes 209
 - trunk groups 209
 - configuring 215

U

- universal power supply 13
- upgrades, performing
 - extracting upgrade files from the download file 313
 - firmware upgrade 315
 - firmware version, verifying 310
 - obtaining the latest upgrade file 312
 - software upgrade 320
 - software version, verifying 310
 - upgrades and configuration files 316

- when to perform 316
- UPkts 293
- Upload Configuration 161, 163

V

- V.35 LED 12
- voice jitter 37
- Voice over IP
 - implementing 84
 - packetized voice 37
 - QoS transitioning technology 39

W

- wall mounting
 - installing 108–110

PERMIT TO OCCUPY
THE LAND OF THE STATE OF TEXAS

By and for the State of Texas, I, the undersigned, do hereby certify that the above named person or persons are entitled to occupy the land described in the foregoing certificate of title, and that the same is not subject to any other claim or lien.

Witness my hand and seal of office at Austin, Texas, this _____ day of _____, 19____.

Notary Public in and for the State of Texas, my commission expires _____ day of _____, 19____.

My commission expires _____ day of _____, 19____.

My commission expires _____ day of _____, 19____.

My commission expires _____ day of _____, 19____.

Notary Public in and for the State of Texas, my commission expires _____ day of _____, 19____.

NOTARY
NETWORKS

Remote Office 9150

Installation and Administration Guide

Copyright © 2001 Nortel Networks, All Rights Reserved.

Printed in Canada.

All information contained in this document is subject to change without notice. Nortel Networks reserves the right to make changes to equipment design or program components, as progress in engineering, manufacturing methods, or other circumstances may warrant.

*Nortel Networks, the Nortel Networks logo, the Globemark, Unified Networks, Meridian 1, Succession Communication Server for Enterprise 1000, and MSL-100 are trademarks of Nortel Networks.

PROCOMM PLUS is a trademark of Datastorm Technologies, a subsidiary of Quarterdeck Corporation.

MICROSOFT, MS-DOS, WINDOWS, and WINDOWS NT are trademarks of Microsoft Corporation.

Product release:	1.3.0
Publication number:	555-8421-215
Document release:	Standard 2.0
Date:	September 2001

NORTEL
NETWORKS™